改訂新版

類体論へ至る道

初等数論からの代数入門

足立恒雄



日本評論社

序

本書は,『数学セミナー』誌に 1 年間 (1978 年 6 月号〜1979 年 5 月号) 連載したものを修正・加筆したものである.

現代数学の特色はその抽象性にある. この抽象性が数学を難解で近寄り難い, かつ索漠としたものに思わせる最大の原因になっている. 専門家と非専門家との間にある断絶を, 整数論という幾分かは馴染み易い分野を通じて埋めようというのが本書の目的とするところである.

数学における抽象化の手段は大きく分けて二種類ある. その一つは本書の主題の一つである同一視という手段である. これはまた類別という形で登場する. たとえば, 1 という数そのものが, 色々の 1 個の物の総体に付された名称であると考える時, 同一視, 乃至, 類別は数学における基本的概念であるのみならず, 人間の本源的に有する基本的能力だということがわかるだろう. つまり, 犬, 人間といった類を表す手法を素材として同値類別という数学的概念が切り出されたのである.

第二の抽象化は極限という手段によって行われる. 同一視が代数学を特徴付けるものとするなら, こちらは解析学を特徴付ける概念である. しかし, 極限という手法も数学の専売特許なのではなく, 人間の本来有する根源的能力が数学という場に先鋭な形で現象しているというに過ぎない.

たとえば,「美」という概念を例にとろう. A さんと B さんでは A さんの方が美しい, C さんと D さんとは比較しがたい, といった不等号の総体の成す射影極限が「美人」という抽象概念であると考えられる.「美人」そのもの

という存在はない．このようにある種の不等号の総体によって新しい極限的存在を創造するのが極限という手法である．

その他に「理想元の追加」という第三の手法がある．これは神様が存在すると仮定すると万事うまく説明がつく，というのと似た話だが，数学的にはコンパクト化という手法がこれにあたる．

数学を数学たらしめている抽象性というのは，単に抽象的ということよりもむしろこれらの抽象化の手段を何度も反復使用することに本質的に意味がある．数学以外の世界では，種々の「美」の概念，「美 1」，「美 2」，からさらに抽象化を行って新概念を創出するというような作業は通常行わない．しかし数学では $1, 2, \cdots$ から整数，整数から有理数，有理数から実数，といった具合に何度も類別および極限という手段を用いて抽象化が行われるのである．このこと，即ち抽象化が再三行われるという数学の本質が数学を敬遠させる本当の理由なのである．

本文中に述べたように，反復によって抽象存在は具体的存在と化するのであるから，反復練習以外に数学における抽象をわが物とする道はないが，ものには方便ということがある．本書が初心の学生，巷間の愛好家の，数学，および数学の世界を知りたい，肌で触れてみたいという願望によく応えるものかどうかは覚束ないが，目的とするところは先に述べたように整数論を方便として抽象を抽象と感じなくさせようということにある．

昭和五十四年 盛夏　　著者識

改訂新版序

私が最初に書いた本である『類体論へ至る道』を復刊する話をいただいたとき，最初の数章を読んで，結構面白いところもあるから，これなら (ちょっと気恥ずかしいようなところもあるが) そのまま手直しなしで復刊しても良いかなあ，という気になり，お引き受けした．ところがこれが間違いの元というか，きっかけを得たというか，大改訂に踏み込み結局は全面的に書き下ろすのと同じ位手間がかかる結果になった．

第 5 章位までは大した修正もなしに済ませたのだが，後半に入ると，そもそも証明がほとんどないまま話がどんどん高度になっていくところが気に入らない上，大して関係もない数学的話題が次々うわべだけの紹介で登場するのも，薄っぺらな感じがしてやりきれない気がしてきた．雑誌の連載では良いことでも，一巻の書物としては具合が悪いのである．どうするか迷ったのだが，証明 3 割，お話 7 割だったのを，証明 7 割，お話 3 割という感じにして数学的に他書を参照しなくても良いようにすること，関係のない話題は削る，樹木で言えば，剪定を行って，見通しを良くすること，を目指して書き直すことにした．主題はほとんど変更しなかったが，数学的な厳密性についてはかなりの程度改善したと思う．とりわけ，集合論の基礎を補強することによって，本全体のグラグラした印象を拭い去ることができたと思う．

こうした作業によって，改訂版と言っても，半分以上書き直したので，30 歳若い自分との共著のような珍しい本になってしまったという印象が深い．

なお，数学的な話題は削ったが，雑談は半分ほど残した．これまで削ると

まったく別の本になるから雰囲気だけでも残す方が良いと思ったのと，こうした息抜きは，固い内容の本としては珍しいと考え，気恥ずかしいようなことが書かれているとは思うが，若かったころの記念として留めておくことにした．アホなことがいっぱい書いてあるなあと思うがまあ良いでしょう．

しかし，30 年前の初版のころならともかく，2009 年の現在となっては雑談で触れられている倉田令二朗さんを始めとする人たちについて聞いたことがないという読者も数多いことだろう．それを考えて，特別付録として，倉田令二朗さんへの追悼文「赤々と沈みゆく太陽を見る」を『万人の学問をめざして』(日本評論社刊) から転載させていただくことにした．併せて読んでいただければ，雑談がどういう背景の下に書かれているか，どう古き良き時代であったのか，おぼろげながらもわかっていただけるだろう．

もし全体を読み通すことができれば，続いて，高木『代数的整数論』へと何の困難もなく進めるであろう．3 割方は内容を知っていないと数学の本は読めないが,『代数的整数論』の結果だけなら，その大半を，また証明を含めてなら半分位は知っていることになるからである．

この改訂新版を木下素夫，杉浦光夫，倉田令二朗の三人の先輩の霊前に捧げる．今日あるのは三人の先輩のおかげだと思っているので感謝の印のつもりである．

なお，原稿を読んで誤りを匡して下さった方々にお礼を申し上げる．とりわけ，尾崎学さんには 11 章以降，また上江洲忠弘さんには集合論的な事柄について数多くの貴重なご指摘を頂いた．

2009 年 12 月　　足立 恒雄

目　　次

記号一覧

第1章　1次方程式と
ピュタゴラスの方程式

§1. 群の定義など

群の定義位は仮定して始めたいところだが，入門書としての体裁上，さらにさかのぼって写像の定義から整えていくことにしよう．

定義 (集合の直積)　A, B を集合とする．集合

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

を A と B の直積という．

定義 (写像 (関数))　T が集合 A から集合 B への写像 (あるいは関数) であるとは，

1. $T \subseteqq A \times B$
2. $\forall x\,(\in A)\,\exists y\,(\in B)\,[(x, y) \in T]$
3. $(x, y) \in T \wedge (x, y') \in T \Longrightarrow y = y'$

の3条件が満たされることである．T が A から B への写像であるとき

$$T : A \longrightarrow B$$

と記す．また $(x, y) \in T$ のとき

$$y = T(x)$$

と記す．(ちなみに，$\forall x\,(\in A)\,\exists y(\in B)[\cdots]$ は任意の $x\,(\in A)$ に対して $\cdots$ を満たす $y(\in B)$ が存在する，と読む．)

条件2は T の定義域が A であることを要請している．条件3は x に対して値が一つであること，すなわち T が1価であることを意味している．

この写像の定義に従えば，実数列 $\{a_n\}_{n=1}^{\infty} = \{a_1, a_2, \cdots, a_n, \cdots\}$ は自然数の集合を定義域とし，実数体 (実数全体のなす集合) $\mathbb{R}$ を値域とする写像であると解釈される．また実数値関数と呼ばれているものも $\mathbb{R}$ から $\mathbb{R}$ への写像である．$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ といった置換も集合 $\{1,2,3\}$ から $\{1,2,3\}$ への写像 (とくに1対1写像) であることになる．実に，集合と写像こそは全数学の基盤概念であることが良くわかるであろう．

定義 (全射性・単射性)　写像 $T: A \longrightarrow B$ が全射 (あるいは，上への写像) であるとは B の任意の元が A の元の像となっていることをいう．すなわち

$$\forall y(\in B)\ \exists x(\in A)\ [y = T(x)]$$

の成り立つことである．

写像 $T: A \longrightarrow B$ が単射 (あるいは，1対1の写像) であるとは，

$$T(x) = T(x') \Longrightarrow x = x'$$

の成り立つことをいう．同じことだが，対偶を取って，$x \neq x' \Rightarrow T(x) \neq T(x')$ とした方が意味はわかり易いかもしれないが，証明には上述の方が使い易い．

定義 (群)　G を集合 $(\neq \varnothing)$ とし，$T: G \times G \longrightarrow G$ を写像とする．$T(x,y)$ のことをここでは $x \cdot y$ と記す．次の3条件が満足されるとき G は演算 $\cdot$ に関して**群** (group) をなすという：

1. (結合律)　$(x \cdot y) \cdot z = x \cdot (y \cdot z)$

2. (単位元の存在)　$\exists e(\in G)\forall x(\in G)[x\cdot e=e\cdot x=x]$
3. (逆元の存在)　$\forall x(\in G)\exists y(\in G)[x\cdot y=y\cdot x=e]$

例題　条件 2 で保証された単位元 e は一つしか存在しないことを示せ．

解答　e_1, e_2 を単位元とせよ．すると任意の $x\in G$ に対して

$$x\cdot e_1=e_1\cdot x=x$$
$$x\cdot e_2=e_2\cdot x=x$$

が成り立つ．したがって

$$\begin{aligned} e_2 &= e_2\cdot e_1 \qquad (\text{上の式で } x=e_2 \text{ とする}) \\ &= e_1 \qquad (\text{下の式で } x=e_1 \text{ とする}) \\ \therefore\quad & e_1=e_2 \end{aligned}$$

[注意]　(1)「一つしか存在しないこと」(一意性) の証明を要求されたら，上のように「x_1，x_2 が与えられた性質を満たしているとして $x_1=x_2$ であることを示す」のが鉄則と言って良いテクニックである．

(2) しばしば，x_1，x_2 が与えられた性質を満たす「二つの元」として，$x_1=x_2$ を示し，「故に矛盾．よって $x_1=x_2$」という型の答案をみかける．こういう，必要もないのに背理法を使う証明は「悪しき背理法」と呼ばれて昔からバカにされてきたので注意してほしい．

問題　条件 3 で保証された逆元 y は x に対して一意的に定まることを示せ．

x の逆元 y のことを x^{-1} と記すのが普通である．数であろうと行列であろうと単位元や逆元が一意に定まることが，たった一つの命題で証明されてしまうのが抽象代数学の威力である．

群 G がさらに任意の $x, y\ (\in G)$ に対して

4. (可換性)　$x\cdot y=y\cdot x$

という性質を持つとき，**可換群** (あるいは**アーベル群**) と呼ばれる．

なお群の演算が $+$ で書かれているときは可換性，すなわち $x+y=y+x$，は必ず要求され，その群は**加群**(あるいは**加法群**)をなすというのが普通である．

例　$m \times n$ 行列の全体 $M(m \times n, \mathbb{R})$ は $+$ に関して加群をなす．また有理数の全体も $+$ に関して加群をなす．n 次正方行列のうち正則なもの(言い換えれば，行列式 $\neq 0$ なるもの)の全体を G_m と書くと G_m は乗法に関して群をなすが，これは可換群ではない．

§2. 簡単な不定方程式

一番簡単な不定方程式は

$$ax + by = c \quad (a, b, c \in \mathbb{Z}) \tag{1}$$

であろう．(ここで $\mathbb{Z}$ は整数全体を表す．したがって(1)の後半の $a, b, c \in \mathbb{Z}$ は a, b, c を整数とする，という意味である．また自然数の全体は $\mathbb{N}$ で表す．)

しかしながら歴史に登場した順序で言えば，2次の不定方程式

$$x^2 + y^2 = z^2, \qquad (x, y) = 1 \tag{2}$$

の方がはるかに古い．それは(2)がご承知のように幾何学的な意味を持っているからで，今も昔も土地所有が人の重要関心事であることを暗示しているのだろうか．

(1)には少なくとも一見異なった解法が3種類ある．一つは純然とユークリッドの互除法を全面に打ち出す初等整数論的手法であり，もう一つはイデアルという概念を導入するものであり，最後の一つは群の概念を用いる方法である．このいずれも本書で取り上げるが，これら3種の証明は本質的には次に述べる $\mathbb{Z}$ における割算の原理を基としている．

定理 1.1 (割算の原理)　a, b を整数とし，$b \neq 0$ とすると，

$$a = qb + r, \quad 0 \leqq r < |b|$$

を満たす整数 q, r が存在する．

この定理を既知としよう．$\mathbb{Z}$ を b の倍数で分割すればよいのである．整数の，ひいては代数の基本的な問題の多くは，この割算の原理に還元されるのだが，問題に向かったとき既知のはずのこの定理が真先に頭に浮かぶ学生というのはかなり少数である．たとえば G を群とし，$g \in G$ としよう．$g^n = e$(単位元) を満足する自然数 n があったとして，その最小のものを n_0 とする．すると $g^n = e$ なる自然数 n はすべて n_0 の倍数である．これを証明せよと要求されたとき，大学に入って群論を習い始めたばかりの段階では，たとえば早稲田の数学科で言えば正解者は 5% くらいである．そんな馬鹿なと思われるかもしれないが，これが現実なのだ．だからこれも定理として後の使用のために書いておこう．

定理 1.2　g を群 G の元とする．

$$g^n = e \qquad (\text{単位元}) \tag{3}$$

を満たす自然数 n が存在するとして，そういう最小の自然数を n_0 とする．すると，(3) を満たす n はすべて n_0 の倍数である．n_0 を g の**位数**という．

証明　$n = qn_0 + r$，$0 \leqq r < n_0$ を満たす整数 q, r を取る．

$$e = g^n = g^{qn_0+r} = (g^{n_0})^q g^r = g^r \quad (\because g^{n_0} = e)$$

$$\therefore \quad g^r = e, \quad 0 \leqq r < n_0$$

n_0 の選び方 (最小性) から $r = 0$．$\therefore \quad n_0 | n$　∎

なお，g^n は g を n 回かけ合わせたものとして定義される．正確に言えば，$g^0 = e, g^{n+1} = g^n \cdot g$ によって回帰的に定義される．

$n_0 | n$ は n が n_0 で割り切れること (n は n_0 の倍数であること) を意味する記号である．このことはまた $n \equiv 0 \pmod{n_0}$ とも書かれる．

問題　G が有限群，すなわち群 G が有限集合とすると各々の $g(\in G)$ に対して $g^n = e$ となる自然数 n は必ず存在する．

[ヒント]　$g, g^2, \cdots$ を考えよ．

さて，$x=3$，$y=4$，$z=5$ が (2) の解であることは人類の文化史と同じだけ古くから知られていたが,

$$dx = a^2 - b^2, \quad dy = 2ab, \quad dz = a^2 + b^2 \quad (a, b \in \mathbb{Z}) \tag{4}$$

(ここでは d は $(x, y) = 1$ となるように選ぶ) が (2) のすべての整数解を与えることも少なくとも今から 4000 年近い昔から知られていた．

(4) という解は完全である．(4) の (x, y, z) はすべて (2) の解であり，逆に (2) の解はすべて (4) の形に表せるのだから．しかし不定方程式がこうした意味で完全に解かれることはごく稀だということを注意しておく．

1 次不定方程式 (1) が実は単一の原理で解かれるのだと言ったが，(2) は一応は異なった立場からの解法が 3 種類ある．いずれも群の概念に関係なくて，途中で述べると宙に浮いた感じがするという理由で，まずこちらから先に片付けよう．

第 1 の解法　有理数体 (有理数の全体) を $\mathbb{Q}$ で表す．(2) を解くことは次の (5) を解くことと同値であることは明らか：

$$x^2 + y^2 = 1 \quad (x, y \in \mathbb{Q}) \tag{5}$$

円 (5) 上の点 $(-1, 0)$ を通り，傾きが有理数 t の直線

$$y = t(x+1)$$

を考える．この直線と円 (5) とのもう一つの交点は 2 次方程式の理論から必ず有理点，すなわち $x, y \in \mathbb{Q}$ なる点である．実際，方程式を解くと

$$x = \frac{1-t^2}{1+t^2}, \qquad y = \frac{2t}{1+t^2} \tag{6}$$

を得る (円のパラメトリゼーション)．$x \in \mathbb{Q}$, $y \in \mathbb{Q}$ より

$$t^2 = \frac{1-x}{1+x} \in \mathbb{Q} \qquad \therefore \quad t = \frac{1}{2} y(1+t^2) \in \mathbb{Q}.$$

そこで $t = b/a$，$a, b \in \mathbb{Z}$ と表すと，

$$x = \frac{a^2 - b^2}{a^2 + b^2}, \qquad y = \frac{2ab}{a^2 + b^2}$$

x, y を $x/z, y/z$ $(x, y, z \in \mathbb{Z})$ と書くと

$$\frac{x}{a^2-b^2}=\frac{y}{2ab}=\frac{z}{a^2+b^2}$$

この比の値は有理数だから $\dfrac{k}{d}, (d,k)=1$ と置いて

$$dx=k(a^2-b^2), \quad dy=k\cdot 2ab, \quad dz=k(a^2+b^2).$$

x, y は互いに素だから $k=1$ で (4) を得る．

(5) を曲線という立場でながめると，いわゆる有理曲線である．すなわち，(6) のような有理式によるパラメータ表示ができる．しかしながら有理曲線だからといっても，いつでも (6) のような有理係数の有理式で表示できるとは限らないから，2 次不定方程式 (2) が今のようにして解けるのはやはり稀なのだ．それにしてもこの第 1 の解法は幾何学的な解法と言えるだろう．このように，2 次曲線上で一つ有理点がわかっていれば，他の有理点は簡単に求まる．この方法を用いて次の問題を試みよ：

問題　次の不定方程式の整数解をすべて求めよ：

1. $x^2+2y^2=z^2$ (さらに $x^2+my^2=z^2$)
2. $x^2+y^2=2z^2$
3. $x^2+y^2=mz^2$ を，1 組の解が知られているとして解け．

第 2 の解法　これはどの本にも出ている初等整数論的な解法なので，説明は少し簡略にしてもいいだろう．

x, y がともに奇数ということはありえないから y が偶数とする．

$$y^2=z^2-x^2=(z+x)(z-x), \quad (z-x, z+x)=2$$

したがって，$z+x=2Y^2$，$z-x=2X^2$ を満たす整数 X, Y が存在する．

$$\therefore \quad x=Y^2-X^2, \quad y=2XY, \quad z=X^2+Y^2$$

[注意]　y が偶数と決めたので上の形になる．(4) は y が偶数とは限定していない．

a, b が整数のとき記号 (a, b) は a, b の最大公約数を表すことはご承知の通

り．上の証明で素因数分解の一意性が使われていることもご承知の通り．もしかしてご承知でないと困るのでやっぱり書いておこう．

問題　$a, b \in \mathbb{N}$ とする．$(a, b) = 1$ かつ ab が平方数ならば a, b はともに平方数であることを示せ．

[ヒント]　次の定理を使う．

定理 1.3 (初等整数論の基本定理)　合成数は素数の冪積に分解することができ，しかもその分解の結果はただ一通りである．

この定理はいかにも自明そうだが証明するとなると割りにめんどうだ．というよりは何をどう証明したら良いかわからない．何故こんな物が基本定理なのかは，この定理が成り立たないような，つまり素因数分解の一意性が成り立たないような例を知らないと理解できないので証明は後回しにしよう．

序文にも触れたことだが，一見自明な事柄，ないしは無意識的に知っていることを分析して原理なり，定理なりに意識化・顕在化するのは他の学問と同様，数学においても大変重要であり，また困難なことである．たとえば，背理法とか三段論法とか対偶というのは簡単な場合には無意識に，あるいはその場その場で考えるなりすれば理性ある人には自明な論理かもしれないのだが，論証というものを分析していくつかの基本的な推論に分解できることを示したギリシア人は称えようもないほど偉大だと思う．偉大である証明には，論理がうまく分析されていない例をあげるのがよかろう．

> 司馬牛，君子を問う．子曰く，君子は憂えず，懼(おそ)れず．曰く，憂えず，懼れずば，これを君子と謂うべきか．子曰く，内に省みて疚(やま)しからざれば，それ何をか憂え何をか懼れん．(『論語』，第十二・顔淵篇より)

司馬牛は逆の命題を持ち出して逆ネジを喰らわせたのである．孔子の答はあいまいで直接の答にはなっていない．もし孔子が「逆必ずしも真ならず」と

いう超論理的命題を知っていれば，ちがった答え方をしたのではなかろうか．

論語が出たついでに，老子からも有名な対句を引いてバランスを取ろう．

> 信言は美ならず，美言は信ならず．善なる者は弁ぜず，弁ずる者は善ならず，知る者は博からず，博き者は知らず．

これは対偶を並べているのだから，論理的には半分のスペースに縮められる．ただ，読んだ瞬間は信言 (真言) と美言とがある種の必要十分条件であるかの如き感触も与えるのでただ重複しているとは言い難い．老子も対偶だから当然成り立つのだとは考えていないように思われる．

基本となる推論形式はすべてギリシア時代に発見されているが，ただ一つ数学的帰納法は例外で，これはパスカルによって定式化された．パスカルの神秘 6 角形というギリシア幾何学的命題とあわせて考えるに，パスカルというのは正しくギリシア以来の大天才なのだということが納得されよう．

第 3 の解法　これは代数的整数論の初歩的手法で，(2) を

$$(x+iy)(x-iy)=z^2$$

と分解する方法である．しかるに，$a+bi$ $(a, b \in \mathbb{Z})$ の形の数全体に対しても素因数分解ができるのだろうか．大体，$a+bi$ が素数って何だ？　こういうわけでこの方法は現在の段階では先に進めない．数章後に扱うであろう (第 5 章 §3 参照)．この手の手法はフェルマー予想にもある種の暗示を与えるが，これについても後に触れる．

§3. 1次不定方程式

m を $m>1$ なる自然数として固定する．a を整数として，$a+km, k \in \mathbb{Z}$ と表せる整数の全体を，$\overline{a}$ あるいは $a \bmod m$ と表す：

$$\overline{a} = a \bmod m = \{a+km \mid k \in \mathbb{Z}\}$$

すなわち，m で割った余りが，a を m で割った余りと等しい整数の全体を $\overline{a}$ と記すのである．こういう $\overline{a}$ は一つの m に対して有限個しかない．それは，

$\overline{0}, \overline{1}, \cdots, \overline{m-1}$ である．集合 $\{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ を $\mathbb{Z}/m\mathbb{Z}$，あるいは $\mathbb{Z}/(m)$ と書くことにする．$\mathbb{Z}/m\mathbb{Z}$ に $\mathbb{Z}$ の加法・乗法を遺伝させることができる．すなわち

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}$$

によって $\mathbb{Z}/m\mathbb{Z}$ の元の間に加法と乗法を定義する．$\mathbb{Z}/m\mathbb{Z}$ の元といっても，たとえば $\overline{0}$ は集合 $\{0, \pm m, \pm 2m, \cdots\}$ であるが，それを一つの元とみなしているところに妙味がある．丸っきりの初心者には最初は理解しにくいところである．しかし実はこうした考え方は第3章で述べるように幼少の頃からすべての人がたたき込まれた人類固有の (に思える) 発想の一種なのであって，これも一種の意識の顕在化なのだ．だからくり返し反復練習することによって何ら異質な発想でないことが理解される．そしてついには，良い意味でも悪い意味でも当たり前のような気がしてくる．

> 抽象的存在は反復によって具体的存在と化する．(足立恒雄名言録より)
>
> 具体的概念は本来抽象的存在なのだ．それを忘却すると概念は「明白」と「難解」に截然と分類される．(同)

$\mathbb{Z}/m\mathbb{Z}$ はこの加法と乗法で閉じているわけだが，加法では群をなし，また乗法については結合法則，そして分配法則を満足するから，いわゆる環である．

環の定義を掲げる前に，再度論理記号について記しておく：

$\forall x \varphi(x)$ は「任意の x に対して $\varphi(x)$ が成り立つ」と読む．また $\exists x \varphi(x)$ は「$\varphi(x)$ を満たす x が存在する」と読む．

長々しい記述がこの程度の記号の導入でかなりの程度短縮されてしまうのだから，便利でもあるが，不思議でもある．数学における闘いの半ばは良い記号の発明にある，とはラプラスの言葉だが $\forall$ や $\exists$ の記号 (あるいはそれと同等の記号) を発明した人は偉い人に違いない．

定義　二つの演算 $+$ と $\cdot$ を持つ集合 R がそれらの演算で閉じており，次

の諸条件を満たすとき，**環** (ring) をなすという：

1. R は $+$ で加群をなす.
2. 乗法に関して結合法則が成り立つ：
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
3. 分配法則が成り立つ：
$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

整数の全体 $\mathbb{Z}$ や $\mathbb{Q}$ や実数体 $\mathbb{R}$ が環をなすことはよく知られている．$\mathbb{Z}$ は有理整数環という名で知られる．いつまでも整数の全体などと言っていないで，**有理整数環**と呼べば,「オッ，できる！」と尊敬を勝ち得ること疑いなし．実数を成分に持つ 2 次の正方行列の全体 $M_2(\mathbb{R})$ も行列の加法と乗法で環をなす．ただし，$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ は

4. $a \cdot b = b \cdot a$

という可換法則を満たすが $M_2(\mathbb{R})$ は満たさない．また以上のすべての環は

5. $\exists e\,(\in R)\ \forall a\,(\in R)[e \cdot a = a \cdot e = a]$

を満足している．$M_2(\mathbb{R})$ では単位行列が e の役割を果している．e は R の (乗法) 単位元と呼ばれる．本書では 1. から 5. までのすべてを満たす環しか扱わないから，こういう環を単に環と呼ぶことにしよう．その正式名称は「単位元を持つ可換環」である．

さて，たとえば $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$　$\therefore$　$\overline{a} + \overline{0} = \overline{a}$ 等によって，$\mathbb{Z}/m\mathbb{Z}$ が環をなすことが知られる．乗法単位元は $\overline{1}$ である．$\mathbb{Z}/m\mathbb{Z}$ は $\mathbb{Z}$ や $\mathbb{Q}$ と違って有限集合である．すなわち有限環である．$\mathbb{Z}/m\mathbb{Z}$ の元は剰余類とも呼ばれる．$\mathbb{Z}/m\mathbb{Z}$ を m を法とする**剰余 (類) 環**と呼ぶ．

$\mathbb{Z}/m\mathbb{Z}$ の元のうち, m と素な整数からなる類の全体を $(\mathbb{Z}/m\mathbb{Z})^\times$ と表そう：
$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\overline{a} \mid (a, m) = 1\}$$

例　$m=6$ とすると $(\mathbb{Z}/6\mathbb{Z})^{\times}=\{\overline{1},\overline{5}\}$．なぜならば，たとえば $(2,6)\neq 1$．$\therefore$ $\overline{2}\notin(\mathbb{Z}/6\mathbb{Z})^{\times}$，また $(3,6)\neq 1$．$\therefore$ $\overline{3}\notin(\mathbb{Z}/6\mathbb{Z})^{\times}$．また $6k+1$ の形の数は 6 と互いに素だから $\overline{1}\in(\mathbb{Z}/6\mathbb{Z})^{\times}$．$\overline{5}\in(\mathbb{Z}/6\mathbb{Z})^{\times}$ も同様．

問題　$(a,m)=1$ ならば $\overline{a}$ のどの元も m と素であることを示せ．

$(\mathbb{Z}/m\mathbb{Z})^{\times}$ は乗法の演算で群をなす．たとえば上例で言えば $\overline{5}\cdot\overline{5}=\overline{25}=\overline{1}$ であるから $\overline{5}$ の逆元は $\overline{5}$ 自身，$\overline{1}$ が単位元である．

定理 1.4　G を乗法の演算 $\cdot$ で閉じた有限集合とする．単位元 e が存在し，かつ結合法則が満たされ，さらに

$$a\cdot b=a\cdot c\Longrightarrow b=c \tag{7}$$

が成り立つならば G は群をなす．すなわち逆元が存在する．

証明　$a\in G$ に対し集合 $\{a^n\mid n=1,2,3,\cdots\}$ を考える．これは G の部分集合であるから有限集合でなければならない．したがって，$a^n=a^m$ を満たす相異なる m,n が存在するはずである．$m>n$ としよう．

$$a^n\cdot e=a^n\cdot a^{m-n}$$

仮定 (7) から $a^{m-n}=e$.

$$\therefore\quad a\cdot a^{m-n-1}=e$$

ゆえに a^{m-n-1} が a の逆元である．‖

系 1　$(\mathbb{Z}/m\mathbb{Z})^{\times}$ は乗法で群をなす．これを法 m の**既約剰余類群**という．

証明　まず乗法で閉じていることを示す．$\overline{a},\overline{b}\in(\mathbb{Z}/m\mathbb{Z})^{\times}$ ならば $(a,m)=(b,m)=1$.

$$\therefore\quad (ab,m)=1,\qquad \therefore\quad \overline{a}\overline{b}=\overline{ab}\in(\mathbb{Z}/m\mathbb{Z})^{\times}$$

次に $\overline{a}\cdot\overline{b}=\overline{a}\cdot\overline{c}$，$\overline{a},\overline{b},\overline{c}\in(\mathbb{Z}/m\mathbb{Z})^{\times}$ とすると

$$ab\equiv ac\pmod{m}\qquad \therefore\quad a(b-c)\equiv 0\pmod{m}$$

$(a, m) = 1$ だから，$b - c \equiv 0 \pmod{m}$　$\therefore\ \bar{b} = \bar{c}$.

結合法則は $\mathbb{Z}/m\mathbb{Z}$ が既にこれを満たすから調べる必要がない．‖

問題　1. $-\bar{a} = \overline{-a}$

2. $\bar{a} = \bar{0} \Longleftrightarrow a \equiv 0 \pmod{m}$

すでに一部使っている記号ではあるが，改めて定義を与えよう：

定義　$a - b$ が m の倍数のとき

$$a \equiv b \pmod{m}$$

と表し，a は b に m を法として (あるいは mod m で) **合同**であるという．

この定義と上の問題によって

$$\bar{a} = \bar{b} \Longleftrightarrow a \equiv b \pmod{m}$$

がただちにわかる．$a \equiv b \pmod{m}$ とは $a = b + km$ なる $k \in \mathbb{Z}$ が存在することであるが，この k が何なのかは問題にならないことが多いので表面から k を消しているのだ．ラプラスの言葉を待つまでもなく，この記号は素晴らしい記号である．これは $a \equiv b \pmod{m}$ がある意味で a と b とが「等しい」ことを表現しているのに較べ，同じことを表すにも $m|a - b$ はそうではないからである．

系 2　$(a, m) = 1$ のとき，1次合同式

$$ax \equiv b \pmod{m}$$

は解 x を持つ．

証明

$$\begin{aligned} ax \equiv b \pmod{m} &\Longleftrightarrow \overline{ax} = \bar{b} \\ &\Longleftrightarrow \bar{x} = \bar{c}\bar{b} = \overline{bc} \\ &\Longleftrightarrow x \equiv bc \pmod{m} \end{aligned}$$

ここに $\bar{c}$ は $\bar{a}$ の (乗法) 逆元とする，すなわち $\overline{ac} = \bar{1}$. ‖

解が m を法としてただ一つであることも明らかであろう．

問題　$ax \equiv b \pmod{m}$ が解を持つための必要十分条件は $(a, m)|b$ である．

系 3　不定方程式 $ax + by = c$ $(a, b, c \in \mathbb{Z})$ が解を持つための必要十分条件は $(a, b)|c$ である．

証明　$(a, b)|c$ ならば上の問題によって $ax \equiv c \pmod{b}$ が解を持つ．したがって $ax = c + kb$ なる k が取れる．$-k = y$ とすればよい．逆に $ax + by = c$ とし，$m = (a, b)$ とする．$a \equiv 0 \pmod{m}$，$b \equiv 0 \pmod{m}$ だから

$$c = ax + by \equiv 0 \pmod{m} \quad \|$$

系 4　$(a, b) = 1$ なるためには $ax + by = 1$ が整数解を有することが必要十分条件である．

これは今や明らかであるが，系4は特筆大書すべき定理なので記憶されたし．互いに素という「主張」が「方程式」として表現されていることに意味があるのである．

問題　$a \equiv b,\ c \equiv d \pmod{m} \implies a \pm c \equiv b \pm d,\ ac \equiv bd \pmod{m}$

例題　$x^3 + y^3 = z^3$ は $xyz \not\equiv 0 \pmod{3}$ なる整数解を有しない．

解答　$x = 3a \pm 1, y = 3b \pm 1$ としよう．

$$\begin{aligned} x^3 &= 27a^3 \pm 27a^2 + 9a \pm 1 \\ &\equiv \pm 1 \pmod{9} \end{aligned}$$

同様に

$$y^3 \equiv \pm 1 \pmod{9}$$

$\therefore\ x^3+y^3\equiv\pm2,0 \pmod 9$．一方，$z=3c\pm1$ とすれば $z^3\equiv\pm1 \pmod 9$ となり $xyz\not\equiv0 \pmod 3$ なら $x^3+y^3\equiv z^3 \pmod 9$ には解がないことになる．したがって当然 $x^3+y^3=z^3$ にもなり得ない．

問題　$x^5+y^5=z^5$，$xyz\not\equiv0 \pmod 5$ は整数解を有しない．これを示せ．

一般に p を奇素数として

$$x^p+y^p=z^p,\quad xyz\not\equiv0 \pmod p$$

には整数解がないという主張を「フェルマー予想の第 1 の場合」と呼んでいる．$p=3,5$ なら上のように簡単に証明できるが，一般的には容易ではない．代数的整数論を主道具とするかぎり，第 1 の場合，第 2 の場合という場合分けは本質的であったが，ワイルズによるフェルマー予想の証明 (1994 年) は全く別の道具立てを用いたもので，上のような場合分けによらず結果に到達したのであった．

定理 1.5　1 次不定方程式

$$a_1x_1+\cdots+a_nx_n=b \tag{8}$$

が解を持つためには $(a_1,\cdots,a_n)|b$ が必要十分条件である．

証明　(8) が解を持てば $(a_1,\cdots,a_n)|b$ は系 3 の証明と同様にして明らかである．

逆は，数学的帰納法を使う．$(a_1,\cdots,a_n)|b$ と仮定して，$(a_1,\cdots,a_{n-1})=c$ と置けば $(c,a_n)=(a_1,\cdots,a_n)$ により $(c,a_n)|b$. $\therefore\quad cx+a_nx_n=b$ となる x,x_n が存在する．帰納法の仮定から $a_1y_1+\cdots+a_{n-1}y_{n-1}=c$ を満たす $y_1,\cdots,y_{n-1}$ が存在するから $y_jx=x_j\ (j=1,\cdots,n-1)$ と置けばよい．
‖

例題　$2x+7y=5$ の整数解を求めよ．

解答　まず $2x \equiv 5 \pmod 7$ を解く．$x = -1$ が一つの解だから，一般解は $x = -1 + 7k$ である．元の不定方程式に代入して $y = 1 - 2k$．(答) $x = -1 + 7k$，$y = 1 - 2k$ $(k \in \mathbb{Z})$

別解　$7 = 3 \cdot 2 + 1$ だから，$x + 3y = u$ と置くと $2u + y = 5$

$$\therefore \quad y = 5 - 2u,\ x = u - 3y = -15 + 7u\ (u \in \mathbb{Z})$$

この別解の方が古典的な解法で，**ユークリッドの互除法**の応用である．割算の原理 (定理 1.1) によって小さい係数に直すところがミソ．互除法という名のいわれは次の問題を解けばわかる．

問題　$32x + 69y = 1$ のすべての整数解を求めよ．

解答　$69 = 2 \cdot 32 + 5$ だから $x + 2y = u$ と置いて

$$32u + 5y = 1.$$

$32 = 6 \cdot 5 + 2$ だから $6u + y = v$ と置くと

$$2u + 5v = 1.$$

$5 = 2 \cdot 2 + 1$ だから $u + 2v = k$ と置けば

$$2k + v = 1.$$

$$\therefore \quad v = 1 - 2k, \qquad \therefore \quad u = -2 + 5k,$$

$$\therefore \quad y = 13 - 32k, \quad x = -28 + 69k$$

これが答である．

$x + 2y = u$ という変換は，正確には

$$x + 2y = u, \quad y = y$$

という1次変換だから行列で書くと

$$\begin{pmatrix} u \\ y \end{pmatrix} = A_1 \begin{pmatrix} x \\ y \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

である．$|A_1| = -1$ だから $A_1^{-1} \in M_2(\mathbb{Z})$，すなわち A_1^{-1} も整数を成分に持つ2次の行列である．したがって

$$x, y \in \mathbb{Z} \iff u, y \in \mathbb{Z}$$

だから $32x+69y=1$ の整数解を求めることは $32u+5y=1$ の整数解を求めることと同値である．同じことが変換 $6u+y=v$ にもいえて，

$$\begin{pmatrix} v \\ u \end{pmatrix} = A_2 \begin{pmatrix} u \\ y \end{pmatrix}, \quad A_2 = \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix}$$

$|A_2|=-1$． $\therefore\ A_2^{-1} \in M_2(\mathbb{Z})$．そして，$A_2A_1 \in M_2(\mathbb{Z})$．

$$\therefore \quad \begin{pmatrix} v \\ u \end{pmatrix} = A_2 \begin{pmatrix} u \\ y \end{pmatrix} = (A_2A_1) \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\therefore \quad \begin{pmatrix} x \\ y \end{pmatrix} = (A_2A_1)^{-1} \begin{pmatrix} v \\ u \end{pmatrix}$$

さらに

$$\begin{aligned} \begin{pmatrix} k \\ v \end{pmatrix} &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} 13 & 28 \\ 6 & 13 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

結局，$13x+28y=k$，$6x+13y=v$ という1次変換を行なうと，$32x+69y=1$ は $2k+v=1$ という簡単な不定方程式に変換される．さらに，徹底させると $2=2\cdot 1+0$ だから $2k+v=l$ と置けば $l=1$ を得る．

$$\begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} k \\ v \end{pmatrix} = \begin{pmatrix} 13 & 28 \\ 32 & 69 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\therefore \quad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 69 & -28 \\ -32 & 13 \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix}$$

したがって，$13x+28y=k$，$32x+69y=l$ という変換をほどこすと，$l=1$ という l と k との方程式（！）に変換されて解は k が任意，$l=1$．したがって

$$x = 69k-28, \quad y=-32k+13$$

となる．

もしも問題が $64x+138y=a$ $(a\in\mathbb{Z})$ という形であれば，今と全く同じ変換で $2l=a$ となる．ゆえに $2|a$ のときに限り解があることになる．

問題　$SL_2(\mathbb{Z})^{\pm}=\{A\in M_2(\mathbb{Z})\mid |A|=\pm1\}$ は行列の乗法で群をなすことを証明せよ．もちろん，$|A|$ は A の行列式である．

今まで現れた $\begin{pmatrix}1&n\\0&1\end{pmatrix},\begin{pmatrix}n&1\\1&0\end{pmatrix}$ $(n\in\mathbb{Z})$ などの行列が $SL_2(\mathbb{Z})^{\pm}$ の元であることは明らかだが，果たして任意の $SL_2(\mathbb{Z})^{\pm}$ の元がこういう形の行列のいくつかの合成で得られるのだろうか？　答はご想像通り大体 yes である．

まず

$$S=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad T=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

と置くと

$$\begin{pmatrix}1&n\\0&1\end{pmatrix}=S^n,\quad \begin{pmatrix}n&1\\1&0\end{pmatrix}=S^nT,$$
$$\begin{pmatrix}0&1\\1&n\end{pmatrix}=TS^n,\quad \begin{pmatrix}1&0\\n&1\end{pmatrix}=TS^nT\quad(\forall n\in\mathbb{Z})$$

であるから不定方程式を解くとき現れた行列はすべて S と T の合成である．

その他に $U=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad V=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ も $SL_2(\mathbb{Z})^{\pm}$ の元である．

定理 1.6　群 $SL_2(\mathbb{Z})^{\pm}$ は S,T,U,V で生成される．すなわち任意の元がこれらとその逆元の合成によって表せる．

なお，$T^2=U^2=V^2=E$ (単位行列) だから逆元といっても意味があるのは S だけである．

証明は次のヒントをもとに各自考えてください：

$M \in SL_2(\mathbb{Z})^{\pm}$ とする．M に左から $\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ を掛けると M の第 1 行の n 倍を第 2 行に加えた行列が得られ，また M に $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ を左から掛けると M の第 2 行の n 倍を第 1 行に加えた行列を得る．何回かこれらの操作をいろんな n について行うと，互除法によって，しまいに八つの行列 $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$, $\begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}$ のいずれかに落ちつく．これらは T, U, V から合成される．このとき $|M| = \pm 1$ に留意．

具体的な行列について上述の操作をやってみることをお勧めする．

最後に変数が増えても事情は変わらぬことを理解するために，次の問題をやってみること:

問題　$32x + 57y - 68z = 1$ の整数解をすべて求めよ．

解答　表し方はいろいろあるが，たとえば，

$$x = 17s + 22t - 6, \quad y = -4t + 1, \quad z = 8s + 7t - 2 \quad (s, t \in \mathbb{Z}).$$

第2章　論理と集合と フェルマーの小定理

§1. 論理と数学について

高校では四つの論理記号 $\vee, \wedge, \neg, \Rightarrow$ を習った．これらはそれぞれ，「または」(or)，「かつ」(and)，「$\cdots$ でない」(not) および「$\cdots$ ならば $\cdots$ が成り立つ」という具体的意味を持っている．そして論理の命題として，

定理 2.1　A, B, C を命題とするとき

1. $\neg(A \vee B) \equiv \neg A \wedge \neg B$
2. $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
3. $\neg(\neg A) \equiv A$

[注意]　$\equiv$ は論理的に同値を意味する．$\Longleftrightarrow$ と同じ．

などが成り立つことをその意味内容を根拠として教えられた．あたかも，ブタを 1 匹飼っていて，さらにもう 1 匹購入すれば合わせて 2 匹になる．したがって $1 + 1 = 2$ であると小学校で教わるように，である．実際には，現実とは (一応) 何の関係もない数の体系があり，一方，現実 (ブタ) が存在する．ブタの頭数の和に自然数の和が対応すると仮定して数理を応用しているに過ぎないのであって，もしもブタが合わせて 2 匹にならなくっても自然数の体系の真理には何の影響も及ぼさない．たとえば，そんなことがあるかど

うか知らないけれども，仮りにコレラ菌二つが合体して1個のデカコレラ菌になったって，それが $1+1=2$ を否定するものだとは誰も考えない．コレラ菌の「個数」には自然数の加法が適用できないだけである．同じことが論理学と実生活の論理についても言える．論理 (推論) にも実際の思考から抽象化されたいくつかの公理があってそれらから論理上の命題が構成される．

たとえば，定理 2.1 にある $\neg(\neg A) \equiv A$ を例に採ろう．A を「私は美しい」という主張とすると $\neg A$ は「私は美しくない」である．しかし $\neg(\neg A)$ は何だろう．まさか「私は美しくなくはない」ではなかろう．実際には，自然言語では $\neg(\neg A)$ を表現する言葉はないのである．これを A とするのは公理であって，本当は定理ではない．

われわれの数学は目的に応じて数学的公理を設定し，定理 2.1 が成り立つような論理体系を推論方式として採用した論理的建築物なのだ．違う論理体系を採用すれば，違う数学ができ上る．数学の分野・目的によってはやや異なる論理体系を用いる必要が実際に生ずる．

定理 2.1 の $\vee$ と $\wedge$ とを入れ換えるともう一つの論理上の命題が得られる：

定理 2.1*

(1)* $\neg(A \wedge B) \equiv \neg A \vee \neg B$

(2)* $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

(3)* 3 には $\wedge, \vee$ が現れないから，$(3)^* = (3)$ である．

さて，大学に入ると数学上必要な論理記号があと二つ導入される．$\exists$ と $\forall$ である．$\vee$，$\wedge$ 等だけでは数学にならないからねえ．

$A(x)$ を変数 x に関する命題 (論理式) とする．$\forall x A(x)$ は「任意の x に対して $A(x)$ が成り立つ」という意味内容を持っている．$\exists x A(x)$ は「$A(x)$ を満たす x が存在する」という意味内容を持つ記号である．このとき

定理 2.2　$\neg(\forall x A(x)) \equiv \exists x \neg A(x)$

$$\neg(\exists x A(x)) \equiv \forall x \neg A(x)$$

の成り立つことが，その意味内容から確かめられる．あるいは定理 2.2 のような単純な論理はすべて公理と考えて差しつかえない．

なお第 1 章で導入した $\forall x(\in S)P(x)$ は S を集合として $\forall x(x \in S \Longrightarrow P(x))$ を簡単に表す (省略的) 記号である：

$$\forall x(\in S)P(x) \equiv \forall x(x \in S \Longrightarrow P(x))$$

同様にして $\exists x(\in S)P(x)$ を

$$\exists x(\in S)P(x) \equiv \exists x((x \in S) \wedge P(x))$$

と定義する．また，命題 A, B に対して

$$(A \Longrightarrow B) \equiv \neg A \vee B \tag{1}$$

と定義する．

注　(1) の両辺の意味が少し異なると感じる人が多い．しかしながら $A \Rightarrow B$ を証明するために，A であるのに $\neg B$ と仮定して矛盾を導き，これで証明ができたとすることには異和感がないだろう．(1) の右辺の否定が $A \wedge \neg B$ なのだから，実際には誰もが (1) を認めているのである．

例題　次を示せ：

$$\neg\,(\exists x\,(\in S)\,P(x)) \equiv \forall x(\in S)\neg P(x),$$
$$\neg(\forall x(\in S)P(x)) \equiv \exists x(\in S)\neg P(x)$$

解答
$$\begin{aligned}\neg(\exists x(\in S)P(x)) &\equiv \neg\,(\exists x\,((x \in S) \wedge P(x)))\\ &\equiv \forall x\neg((x \in S) \wedge P(x)) \qquad (\text{定理 2.2 より})\\ &\equiv \forall x(\neg(x \in S) \vee \neg P(x)) \qquad (\text{定理 2.1}^* \text{ より})\\ &\equiv \forall x(x \in S \Longrightarrow \neg P(x)) \qquad ((1) \text{ より})\\ &\equiv \forall x(\in S)\neg P(x)\end{aligned}$$

第 2 式は各自試みよ．

今後まぎれのない限り，たとえば $\neg(\exists x P(x))$ は $\neg\exists x P(x)$ というようにカッコを略す．また，$\exists x\exists y(\in S)P(x,y)$ によって $\exists x(\in S)(\exists y(\in S)P(x,y))$ を表すなどの簡略化された記号を適宜に使う．

例題　$n\ (\geqq 3)$ を自然数とする．

$$\forall x\forall y\forall z(\in \mathbb{N})(x^n + y^n \neq z^n)$$
$$\equiv \neg(\exists x\exists y\exists z(\in \mathbb{N})(x^n + y^n = z^n))$$

をこれまでに述べたことを用いて証明せよ．(意味を考えれば，両辺が同一命題を表すことはほとんど明らかで，ともにフェルマー予想を表している．)

解答

$$\neg(\exists x\exists y\exists z(\in \mathbb{N})(x^n + y^n = z^n))$$
$$\equiv \neg(\exists x(\in \mathbb{N})\exists y(\in \mathbb{N})\exists z(\in \mathbb{N})(x^n + y^n = z^n))$$
$$\equiv \forall x(\in \mathbb{N})\neg(\exists y(\in \mathbb{N})\exists z(\in \mathbb{N})(x^n + y^n = z^n))$$
$$\equiv \forall x(\in \mathbb{N})\forall y(z \in \mathbb{N})\forall(\in \mathbb{N})\neg(x^n + y^n = z^n)$$
$$\equiv \forall x\forall y\forall z(\in \mathbb{N})(x^n + y^n \neq z^n)$$

問題　「任意の正数 ε, M に対して適当な自然数 N を取れば $N\varepsilon > M$ とできる」という命題の否定命題を作れ．

[ヒント]　当の命題は

$$\forall\varepsilon\,(>0)\,\forall M(>0)\exists N(\in \mathbb{N})[N\varepsilon > M]$$

と表せる．

今までしばしば命題という用語を使って来たが，ここで命題という言葉が何を意味するのかを簡略に定義しておこう．以下では，x, y 等のアルファベットの小文字は集合を表す．なお，現代数学では $0, 1, 2, \cdots$ といった数も，そして関数も，グラフも，すべて集合として捉えられているから，上の「集合」というのは数や図形などの数学的対象をすべて代表しているものといえる (付録「集合論のイロハ」を参照)．

論理式の定義

(1)　$x = y$, $x \in y$ はともに論理式である．

(2)　φ と ψ とが論理式ならば

$$\varphi \Rightarrow \psi, \quad \varphi \wedge \psi, \quad \varphi \vee \psi, \quad \neg\varphi$$

もそれぞれ論理式である．

(3)　φ が論理式ならば，変数 x に対して

$$\forall x \varphi, \quad \exists x \varphi$$

もともに論理式である．

(4)　以上によって定められたものだけが論理式である．

$\forall x\varphi$ とか $\exists x\varphi$ という形で現れる変数 x は**束縛変数**と呼ばれ，束縛されていない変数は**自由変数**と呼ばれている．自由変数は数学の世界ではパラメータと呼ばれていることが多い．論理式 φ が a を自由変数として持つとき a に関する命題ともいわれる．自由変数を持たない論理式を特に**命題**という．

§ 2.　集合について

つぎは集合の話である．A, B を集合とする．A, B 等を部分集合とするような全体集合 Ω を取って，その中で議論することにしよう．たとえば，自然数だけを対象にしているなら $\Omega = \mathbb{N}$ と選べるし，平面図形を扱っているなら $\Omega = \mathbb{R}^2$ を選ぶことができる．

$$x \in A \cup B \equiv (x \in A) \vee (x \in B) \tag{2}$$

$$x \in A \cap B \equiv (x \in A) \wedge (x \in B) \tag{3}$$

によって集合 A, B の和 $A \cup B$，共通部分 $A \cap B$ を定義する．これはまた，$A \cap B = \{x \mid (x \in A) \vee (x \in B)\}$ 等と表すことはご存じの通り．また

$$x \in A^c \equiv x \notin A (\equiv \neg(x \in A)) \tag{4}$$

でもって A の補集合 A^c を定義する．同じことだが，$A^c = \{x (\in \Omega) \mid x \notin A\}$ である．$\cap, \cup$ を $\vee, \wedge$ と混同してはいけない．ここでは A, B は命題ではなく集合なのだ．したがって次の例題は数学の (集合論の) 命題である．

例題　$(A \cap B)^c = A^c \cup B^c, \quad (A \cup B)^c = A^c \cap B^c$

証明

$$\begin{aligned} x \in (A \cap B)^c &\equiv \neg(x \in A \cap B) \quad \text{by (4)} \\ &\equiv \neg((x \in A) \wedge (x \in B)) \quad \text{by (3)} \\ &\equiv \neg(x \in A) \vee \neg(x \in B) \quad \text{by 定理 2.1}^* \\ &\equiv (x \in A^c) \vee (x \in B^c) \quad \text{by (4)} \\ &\equiv x \in A^c \cup B^c \quad \text{by (2)} \\ &\therefore (A \cap B)^c = A^c \cup B^c \end{aligned}$$

双対性によって $(A \cup B)^c = A^c \cap B^c$ も成り立つ. ‖

この例題はしばしば図で説明されるが，それは暗示 (いわゆる heuristic な説明) であって証明ではない．ブタの匹数と数理の関係と同じで，そういう図ではそれが直感的に成り立つというに過ぎない．

問題　A_j $(j \in I)$ を (全体集合 Ω の部分) 集合族とする．(「集合の集合」という同語反復を忌んで集合系とか集合族と言う.)

$$x \in \bigcup_{j \in I} A_j \;\equiv\; \exists j(\in I)[x \in A_j],$$
$$x \in \bigcap_{j \in I} A_j \;\equiv\; \forall j(\in I)[x \in A_j]$$

と定義する．このとき

$$\left(\bigcup_{j \in I} A_j\right)^c = \bigcap_{j \in I} A_j^c, \quad \left(\bigcap_{j \in I} A_j\right)^c = \bigcup_{j \in I} A_j^c$$

を証明せよ．

[ヒント]　定理 2.2 による．

$I = \{1, 2\}$ のときは上の例題と同一内容を持つことがわかる．

ここで一つ直積の概念を数論に適用してみよう．以下，A が有限集合のとき $|A|$ は集合 A の元の総数を表す．

定理 2.3　m, n を互いに素な自然数とする．写像

$$f : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

を $f(x \bmod mn) = (x \bmod m,\ x \bmod n)$ で定義すれば，f は全単射である．

証明　f の単射性がわかれば

$$\begin{aligned}|\mathbb{Z}/mn\mathbb{Z}| = mn &= |\mathbb{Z}/m\mathbb{Z}| \cdot |\mathbb{Z}/n\mathbb{Z}| \\ &= |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|\end{aligned}$$

であるから，全射性も必然的に従う (下記の有限集合の原理による．)

$$\begin{aligned}
&f(x \bmod mn) = f(y \bmod mn) \\
&\qquad \iff (x \bmod m = y \bmod m) \wedge (x \bmod n = y \bmod n) \\
&\qquad \iff (x - y \equiv 0 \pmod{m}) \wedge (x - y \equiv 0 \pmod{n}) \\
&\qquad \iff x - y \equiv 0 \pmod{mn} \qquad (\because (m,n) = 1) \\
&\qquad \iff x \equiv y \pmod{mn} \\
&\qquad \iff x \bmod mn = y \bmod mn \quad \|
\end{aligned}$$

系 1 (Chinese Reminder Theorem：**孫子の定理**)　$(m, n) = 1$ ならば任意の $a, b\ (\in \mathbb{Z})$ に対して連立合同式

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}$$

は解 x を持つ．解は mn を法とすれば，ただ一つである．

証明　$(a \bmod m, b \bmod n) \in \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ の逆像は上の定理により必ず存在し，しかもただ一つである．‖

単に有限集合の元の個数の比較だけで証明が終わっていることに注目してほしい．第 1 章の，m と素な類の全体 $(\mathbb{Z}/m\mathbb{Z})^{\times}$ が群をなすことの証明は $(\mathbb{Z}/m\mathbb{Z})^{\times}$ が有限集合であるおかげで合同式 $ax \equiv b \pmod{m}$ に解 x が存在することを示す必要がなかったのである．このことは重要だから改めて書いておこう．

有限集合の原理　A, B がともに有限集合とする．$A \subsetneqq B$ かつ $|A| = |B|$ なら $A = B$ である．

なお，系 1 は現代に至って中国では古くから知られていることが判明したため，こういう名称を与えられたのである．その最古の文献は『孫子算経』であるから，孫子の名になじみのあるわれわれとしては「**孫子の定理**」と呼んでも良いのではないだろうか．ところで，最近の数学史研究の成果によってヨーロッパ数学以前にインドや中国などで知られていたことが判明したケースが増えている．2 項係数に関する「パスカルの三角形」はその代表例で，欧米では「パスカルの三角形」という用語は廃語になっていると聞いた．

例題　連立合同式 $x \equiv 1 \pmod{11}$, $x \equiv 2 \pmod{7}$ を解け．

解答　第 1 の式より $x = 11y + 1$ $(y \in \mathbb{Z})$．これを第 2 式に代入して

$$11y \equiv 1 \pmod{7} \quad \therefore \quad 4y \equiv 1 \pmod{7}$$

両辺に 2 を掛けて

$$y \equiv 2 \pmod{7} \quad \therefore \quad y = 7k + 2 \ (k \in \mathbb{Z})$$

$$\therefore \quad x = 77k + 23 \quad (\text{答})\ x \equiv 23 \pmod{77}.$$

問題　$(m_i, m_j) = 1$ $(i \neq j)$ ならば連立合同式

$$x \equiv a_j \pmod{m_j} \quad (j = 1, 2, \cdots, n)$$

は常に解を持ち，しかも解は $m_1 \cdots m_n$ を法とすれば，ただ一つであることを証明せよ．

[ヒント]　定理 2.3 の拡張をせよ．

$\varphi(n)$ を自然数 n を越えない，n と互いに素な自然数の個数とする．これは $(\mathbb{Z}/m\mathbb{Z})^\times$ の元の個数といっても同じである．φ は**オイラー関数**と呼ばれる数論的関数である．

例　$\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$．一般に p が素数ならば $\varphi(p) = p - 1$．

系 2　$(m, n) = 1$ ならば $\varphi(mn) = \varphi(m)\varphi(n)$.

証明　f を定理 2.3 の写像とする．f による $(\mathbb{Z}/mn\mathbb{Z})^\times$ の像がちょうど $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ であることを示せば f が単射であることによって証明が終わる．

$x \bmod mn \in (\mathbb{Z}/mnZ)^\times$ とすると，その定義から

$$(x, mn) = 1 \quad \therefore\ (x, m) = 1,\ (x, n) = 1$$

$$\therefore\quad x \bmod m \in (\mathbb{Z}/m\mathbb{Z})^\times, \quad x \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$$

これで $f((\mathbb{Z}/(mn))^\times) \subseteqq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ がわかった．

次に，$(x \bmod m,\ y \bmod n) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$，すなわち $x \bmod m \in (\mathbb{Z}/m\mathbb{Z})^\times$，$y \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ としよう．系 1 によって，

$$\exists z(\in \mathbb{Z})[z \equiv x \pmod m \wedge z \equiv y \pmod n)]$$

$z \equiv x \pmod n$ かつ $(x, m) = 1$ によって $(z, m) = 1$．同様に $(z, n) = 1$ $\therefore\ (z, mn) = 1 \quad \therefore\ z \bmod mn \in (\mathbb{Z}/mn\mathbb{Z})^\times$．しかも

$$f(z \bmod mn) = (x \bmod m,\ y \bmod n)$$

$$\therefore\ (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \subseteqq f((mn\mathbb{Z})^\times)$$

以上から $f((\mathbb{Z}/mn\mathbb{Z})^\times) = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ が示された．　‖

このように集合 A, B に対して $A = B$ を示すには $A \subseteqq B$ と $B \subseteqq A$ を証明するのが鉄則である．$A \subseteqq B$ は $x \in A \Rightarrow x \in B$ を示せばよい．

問題　p が素数で，$n \in \mathbb{N}$ のとき

$$\varphi(p^n) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$$

[ヒント]　p^n を越えない p の倍数は $kp\ (k = 1, 2, \cdots, p^{n-1})$ である．

この問題と系 2 を組み合わせて次の定理を得る：

定理 2.4　自然数 n の素因数分解を $n = p^a q^b \cdots r^c$ とすると

$$\varphi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\cdots\left(1 - \frac{1}{r}\right).$$

§3. フェルマーの小定理

フェルマーの小定理というのはご存じの読者が多いと思う．p を素数とし，$(a,p)=1$ とすると

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つというのがそれだ．もしくは剰余類を使って書き直せば

$$\overline{a}^{p-1} = \overline{1} \quad (\forall \overline{a} \in (\mathbb{Z}/m\mathbb{Z})^{\times})$$

とも表せる．$\varphi(p) = p-1$ だったから，フェルマーの小定理は次のオイラーの定理の特別の場合である：

定理 2.5 (オイラー)　整数 $m\ (>0)$, a に対して $(a,m)=1$ ならば，

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

あるいは，剰余類で表せば

$$\overline{a}^{\varphi(m)} = \overline{1} \quad (\forall \overline{a} \in (\mathbb{Z}/m\mathbb{Z})^{\times}).$$

$\varphi(m)$ というのは既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^{\times}$ の**位数** (元の総数) だったからオイラーの定理は次の予想を生む：

定理 2.6　G を有限群とする．$|G|$ によって，G の位数を表すと，

$$g^{|G|} = e \quad (\forall g \in G).$$

この予想は正しいので定理とした．e はもちろん G の単位元である．定理 2.6 の証明をするのがこれからの仕事である．

G を群とし，H を G の**部分群**とする．すなわち，H は G の部分集合で，G の演算で群をなすとする．

問題　$H(\neq \varnothing)$ は群 G の部分集合であるとする．H が G の部分群となるためには 2 条件

1. $a \in H \Longrightarrow a^{-1} \in H$
2. $a, b \in H \Longrightarrow ab \in H$

の成り立つことが必要十分条件である．これを示せ．

たとえば G が位数 n の有限群であるとすると，前章で話した通り a の位数とは $a^m = e$ なる最小の自然数 m のことである．$H = \{e, a, a^2, \cdots, a^{m-1}\}$ は明らかに G の乗法で群をなす．したがって H は G の部分群で，その位数は m である．H のように一つの元で生成される，すなわち，一つの元とその冪ですべての元が表される群を巡回群と言うが，巡回群の場合，群の位数は生成元 (今は a) の位数と一致する．

定義　群 G の適当な元 g を取ると

$$G = \{g^n \mid n \in \mathbb{Z}\}$$

と表せるとき, G は**巡回群** (cyclic group), 上のような g は**生成元**と呼ばれる．

例　$\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\}$，すなわちすべての整数は 1 のいくつかの和 (およびその逆元) として表せるから，$\mathbb{Z}$ は加法群と見たとき 1 を生成元とする無限巡回群である．また -1 も生成元である．

H を G の部分群とする．G の 2 元 a, b に対し $ba^{-1} \in H$ が成り立つとき，a は b に同値であると言い，

$$a \sim b$$

と表すことにする．

問題　上の $\sim$ に対して次の三つが成り立つことを示せ：

1. (反射律)　$a \sim a$
2. (対称律)　$a \sim b \Longrightarrow b \sim a$

3. (推移律)　$a \sim b, b \sim c \Longrightarrow a \sim c$

[ヒント]　たとえば $aa^{-1} = e \in H\ (\forall a \in G)$. $\therefore\ a \sim a$.

a と同値な G の元の全体のなす集合は a の属する**剰余類**と呼ばれる．a の属する剰余類，すなわち $\{b(\in G) \mid a \sim b\}$ は Ha と一致する．ここに $Ha = \{ha \mid h \in H\}$ とする．

実際，$b \in Ha$ ならば $\exists h(\in H)[b = ha]$．これより

$$ba^{-1} = h \in H \quad \therefore \quad a \sim b$$

逆に $a \sim b$ とすると定義から $ba^{-1} = h \in H$

$$\therefore \quad b \in Ha$$

定理 2.7　G を群，H を G の部分群とする．G の H による剰余類の全体を $\{Ha_j \mid j \in I\}$ (ただし，$i \neq j$ ならば $Ha_i \neq Ha_j$) とすると，

$$G = \bigcup_{j \in I} Ha_j, \quad Ha_i \cap Ha_j = \varnothing \quad (\text{if } i \neq j)$$

が成り立つ．すなわち G は互いに共通部分がない全剰余類の和集合として表せる．

証明　$Ha_i \cap Ha_j \neq \varnothing$ と仮定すると

$$\exists b(\in G)[b \in Ha_i \cap Ha_j].$$

$b \in Ha_i$ より $b = ha_i(h \in H)$ と表せる．同様に $b \in Ha_j$ より $b = ka_j(k \in H)$ と表せる．故に $ha_i = ka_j$

$$\therefore \quad (k^{-1}h)a_i = a_j, \quad k^{-1}h \in H$$

$$\therefore \quad a_i \sim a_j \quad \therefore \quad Ha_i = Ha_j \quad \therefore \quad i = j$$

次に $b \in G$ とすると，b の属する剰余類 Hb と一致する Ha_i が存在する．

$$b \in Hb = Ha_i \subseteqq \bigcup_{j \in I} Ha_j \quad \therefore \quad G \subseteqq \bigcup_{j \in I} Ha_j$$

逆の包含は明らかだから $G = \bigcup_{j \in I} Ha_j$ が示せた．∥

例　$G = GL_2(\mathbb{R})$，すなわち，G は行列式が 0 でない実数成分の 2 次行列全体のなす群とする．

$$H = \{a(\in G) \mid |a| = 1\},$$

すなわち行列式が 1 の G の元の全体を H とすると，H は G の部分群である．

$a, b \in G$ のとき

$$\begin{aligned} a \sim b &\Longleftrightarrow ba^{-1} \in H \\ &\Longleftrightarrow |ba^{-1}| = 1 \\ &\Longleftrightarrow |a| = |b| \end{aligned}$$

つまり，行列式が一致することが同値の条件となる．したがって $\alpha \in \mathbb{R}^\times$(すなわち $\alpha \neq 0 \wedge \alpha \in \mathbb{R}$) に対し $a_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ と置けば $|a_\alpha| = \alpha$ であるから

$$G = \bigcup_{\alpha \in \mathbb{R}^\times} Ha_\alpha, \quad Ha_\alpha \cap Ha_\beta = \varnothing \quad (\text{if } \alpha \neq \beta)$$

が成り立つ．Ha_α は行列式が α の行列全体のなす集合と一致する．

系 (**ラグランジュの定理**)　G を有限群，H をその部分群とする．$(G : H)$ によって G の H による剰余類の個数 (**群指数**と呼ばれる) を表す．すると

$$|G| = (G : H) \cdot |H|$$

が成り立つ．

証明　全剰余類を $Ha_j (j = 1, 2, \cdots, m)$，$m = (G : H)$ とする．写像 $f : H \longrightarrow Ha_j$ を $f(x) = xa_j$ で定義すると f は全単射である．(これは証明がやさしいから読者に任すことにする.) したがって Ha_j に含まれる元の個数 $|Ha_j|$ は一定で $|H|$ にひとしい．定理 2.7 によれば G はこれら Ha_j の，共通部分のない和として表されるから

$$|G| = |Ha_1| + \cdots + |Ha_m| = m|H| \quad \blacksquare$$

この系から定理 2.6 を導いてみよう．

$g \in G$ とし，g の位数を n とする．H で g の生成する巡回群を表す：

$$H = \{e, g, g^2, \cdots, g^{n-1}\}$$

上の系より

$$g^{|G|} = (g^{|H|})^{(G:H)} = (g^n)^{(G:H)} = e.$$

これでオイラーの定理，したがってフェルマーの小定理が証明されたことにもなる．環・体の話が一通り終わってから再び群の話に戻ってアーベル群の基本定理を述べるが，その折に $(\mathbb{Z}/p\mathbb{Z})^\times$ は実は巡回群であることを証明する．

第3章　類別とイデアル

§ 1. 類別

第 2 章ではフェルマーの小定理のからみで群の剰余類の話が出た．それによると群 G が剰余類と称する部分集合の和集合としてちょうど表されるのであった．これをさらに一般化して次のように考えてみよう．

今集合 S が部分集合系 $\{S_\lambda\}_{\lambda\in\Lambda}$ の和集合としてちょうど表されているとする：

$$S=\bigcup_{\lambda\in\Lambda}S_\lambda,\quad S_\lambda\cap S_\mu=\varnothing\quad(\text{if }\lambda\neq\mu) \tag{1}$$

(1) のような形を集合 S の**直和分割**と呼ぶことが多い．そこで S の 2 元 a,b に対して

$$a\sim b\iff\exists\lambda(\in\Lambda)[a\in S_\lambda\wedge b\in S_\lambda]$$

と関係 $\sim$ を定義する．このとき S における関係 $\sim$ は次の 3 条件 (**同値律**) を満足する：

1. (**反射律**)　$a\sim a$
2. (**対称律**)　$a\sim b\Longrightarrow b\sim a$
3. (**推移律**)　$a\sim b,\ b\sim c\Longrightarrow a\sim c$

問題　上の三つを確かめよ．

逆に，今までのことはご破算にして，集合 S と同値律を満足する S における関係 $\sim$ (**同値関係**と呼ばれる) が与えられたとする．

$$S_a = \{x(\in S) \mid x \sim a\}$$

すなわち，$x \sim a$ という関係にある元 x の全体を一まとめにして S_a と書くことにする．a, b がある同一の S_c に属するとき，かつそのときに限り $a \sim b$ と書くことにするのである．たとえば，日本人の全体の集合を S として，a と b という人が同じ誕生日を持つとき $a \sim b$ と決めると，S_a とは a と同じ月日に生まれたすべての人のなす集合である．

集合 $\{S_a \mid a \in S\}$ を考え，これを S の $\sim$ による**商集合**と呼んで $S/\sim$ と表す．$S/\sim$ の和集合は $\cup\{S_a \mid a \in S\}$ で，これは S である．また $S_a \neq S_b$ ならば $S_a \cap S_b = \varnothing$ であるから，S の直和分割が得られたことになる．なお，$S/\sim$ の各類から代表を選び出して**代表系** (代表の集合) を作るには，一般的には選択公理を要する (第 6 章 §1 の最後の問題参照)．その代表系を $\{a_\lambda\}_{\lambda \in \Lambda}$ とし，S_{a_λ} を S_λ と書けば (1) の形の直和表現を得る．

かくして同値関係 (すなわち条件 1, 2, 3 を満たす関係) と (1) のように部分集合の直和で表現されるということが同等な概念であることがわかった．

[注意]　集合 S と同値関係 $\sim$ が与えられたとして，$S/\sim = \{S_a \mid a \in S\}$ がどうして集合をなすと言えるのか，ということが気になる人がいるかもしれないので一言．以下を読むためには，付録「集合論のイロハ」を予備知識とする必要がある．

まず関係とは集合論の立場で言えば何なのかを定義しなければならない．R が集合 S の**関係**であるとは，$R \subseteqq S^2 = S \times S$ であることを言う．そのとき同値律は

$$(x, x) \in R, \quad (x, y) \in R \Rightarrow (y, x) \in R,$$
$$(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$$

と表現される．$S_a = \{x \in S \mid (x, a) \in R\}$ だから S_a は確かに集合であり，$S_a \in P(S)$ ($= S$ の冪集合) が成り立つ．$S/\sim = \{y\ (\in P(S)) \mid \exists x(y = S_x)\}$

だから，$S/\sim$ は確かに集合である．$y = S_x$ の部分は $\forall z\ (z \in y \Leftrightarrow z \in S_x)$，さらに $z \in S_x$ はその前に論理式で表せている．

今までにも実は何度か同値関係が現れている．たとえば整数 m を法とする合同 $\equiv$ は同値律を満たす．代数学に限らず類別の例を挙げるならば，それこそきりがない．たとえば図形の合同がそうである．平面図形 A, B は平行移動，回転，裏返しを何回か行って重ね合わせられるとき合同というのであった．一辺が 10 cm の正三角形 A を示して，これと同じ三角形を描け，と要求したら誰もがただ一つしか存在しないかの如くにシカツメらしく紙の上に一つ描く．実際には A というのは無数にある合同な三角形のうちの一つに過ぎないのに．

あまり頭の良い子を持っていると気がつかないかもしれないが，3 歳くらいの幼児に「これと同じ図形を描け」と命じたら大抵その意味がつかみかねてボンヤリしているものである．「同じ」という意味が理解できないのだ．だって同じものはただ一つ，そこにしか存在しない！「同じ図形」，「これと同じ物」という意味，つまり合同ということなのだが，それを飲み込むには限りない反復を必要とする．場合によっては「同じ図形」とは相似な図形ということもあるだろう．万人がその苦難を乗り越えられるというのは奇跡としか言いようがないが，これが人間という種の持つ特性なのであろう．

犬はモラルに関しては不思議なほどに人間に似た生き物であるが，犬に「これと同じ形の物を持って来い」という意味を理解させるのは，言葉の障害のせいかもしれないが一般的にはむずかしい (私は種としての能力の違いだと思っている．

関係ないが，犬畜生のような，という言葉は気に入らん．犬は立派な生物なのだが，その最大の悲劇はあきっぽいという決定的な欠陥を持った下司な生物の手下になったことである．ついでだが，昔から私はゴリラとオオカミのファンである．その流れで犬が好きなのだ．だから当然のことながら，超小型犬や人間の手がかかりすぎたケッタイな犬を見ると，これがオオカミの

子孫かと哀れに思う．

さらに余談にわたる．最初にゴリラの本を読んだのは伊谷純一郎さんの『ゴリラとピグミーの森』(1961 年) で，その後上野動物園によくゴリラを見に行ったものだ．最後に読んだのは D. Fossey の自伝 “Gorillas in the Mist” (1983 年) だったと思う (この本を読んで感激し，Digit Fund に 100 ドル寄付したのを思い出した)．オオカミは F. Mowat の “Never Cry Wolf” (1963 年) だった．この本によって世間におけるオオカミの一般的イメージが一変したのである．犬については「オオカミ人間」とも評すべき平岩米吉さんの『犬の行動と心理』(1976 年) が一番良い．最近では彼の伝記が二冊も出ている．オオカミを連れて銀座を散歩したそうだが，だれも気が付かなかったという．動物園のオオカミが傍に寄ってきて金網越しに離れないという話もあって，それ位オオカミに慕われた人だった．

ちなみに，犬に好かれる人と嫌われる人がいるが，どういう判定条件があるのですかね．私はとりわけ犬に好かれる方ではない．単なる観念的な愛好者だからでしょう．一軒家に住むようになってすぐにシェパードを飼い始めた．今は 2 頭飼っているが，こいつら，人間に似て裏表がありましてね．やさしく相手してもらっている間はイイコぶってんですよ．「猫を被る」と言うけど，私の経験から言うと，猫は人間に媚びない．だから本当は「犬を被る」と言うべきでしょうね．

閑話休題．さらに根源に遡れば，数字自身が類別という手段によって抽象化された存在である．誰かが自然数だけが神様が造った数だと言ったそうだが，冗談じゃない，自然数こそは人類が造った最初にして最大の傑作なのである．何か優れたものがあると (言葉のアヤではなくて大真面目に) 神に帰するのは一神教のもたらした疫病ではなかろうか．

ブタ 1 匹も，コレラ菌 1 個も一つという点では同格で一つの部屋に入れられているのである．その部屋が 1 という名前で呼ばれているのだ．(しかし数 1 をこうしたものとして定義しようとすると，$1 \in 1$ といった困難に陥る

が，それはまた別の問題である．)

さらに考察を進めれば，言葉が類別によって作られることを知るだろう．このようにして「類別」という概念は人間の精神およびその歴史の中で最も原初的・根源的な位置を占めていることが理解される．それだけに修得に年月を要する．幼少期の大半をそのことに傾注するといって差しつかえない．翻って大人の目から見て，どうしてこんなことがわからんのかと頭の一つもこづきたくなるのは大抵数や図形に関する事柄であるのを見ても，わかってしまえば当たり前，それまでは五里霧中という数学の持つ性格が本来的なものであることがうかがえるのである．

基本的な概念にもかかわらず，類別という概念が明確に定式化されたのはごく最近のことのようである．(たとえば，高木貞治先生の名著『代数的整数論』において導手の定義がどうもはっきりしないのは同値律が意識的に使われていないからであろう．) 抽象代数が盛んになって商群などから意識的になり，さらに同値律へと進んだのではなかろうか．その目で振り返って見ると，たとえば幾何ベクトルも平行移動して重ね合わせられる矢線の類 (集合) だったことがわかって，向きと大きさを持った何か木の枝みたいなものというあいまいさが払拭された．初めてそれに気がついた人はきっと目からウロコが落ちたような気がしたろう．角度という概念も類別で定義されて初めて人に厳密に伝えられる概念となったと言えるだろう．

類別 (一種の同一視) による抽象化は今ではまったくの常識と化した観さえあるが，その歴史からわかるように決して「当り前」ではないことは認識しておく必要があろう．少なくとも幼い頃にどんなに苦労して類別を修得したかに思いをめぐらせば，子供にヒステリックにならずに済むし，子供も辛い思いをしなくて済む．むしろ，どうしてこんな難解な概念が易々と理解され受け入れられるのだろうかと驚嘆してしかるべきだと常々私は思うのである．もっとも，そんな大英才が成長して整数の合同類別すら理解できないとはこれまた奇妙なことがあるものだとも思う．大人になればなんでも盲目的に吸収してしまう巨大な能力は衰えるから個々の類別に反復によって馴れる

よりは，一般的に同値律を意識的分析的に考察し，逆に過去に修得した，たとえば図形の合同・相似が同値関係であったことに思いをめぐらすのが修得の一番良い方法だと思う．

犬は相似形からの連想を持たないように見える．等身大の像 (鏡・彫刻・写真・絵等) に対してはしばらくの間本物とまちがえることがある．しかし縮小されたそれに対しては決して関心を示すことがない．あれだけ帰主本能の強い犬のことだから旧主の像を見れば懐旧の念を抱くのではなかろうかと思うかもしれないが，そうした例はないのである．犬と人では同じ物に対しても大きく異なった感じ方をしているのであろう．

解剖学を専攻している人に「今さら人間を解剖して何を見ることがあるのですか」と質問してみた．そうしたら，時代によって見えようが違うのですという答が返って来た．なるほどと思った．そう見ようと思って見るのでなければ決してそうは見えないのである．

人にはあるがままに物を見ることなどできないのである．巨大な歴史と文化を背負っている分だけ物のある一面が際立って見えるのである．あるがまま見るということは何も見ないということである．

栄西は道元の問にこの世には石ころと狐狸しか存在しないと答えたというが，何か関係のあることであるようにも受け取れる．

以上は初版時に書いたものだが,最近これを立証するドキュメンタリー『46 年目の光』(NTT 出版) という本を読んだ．3 歳で失明し，46 年経って目が見えるようになった人の話である．この人にはいわゆる図形の錯視は起こらないし，物が立体的に見えることもないし，知らない物は見えないからスーパーの棚は色がにじんで見えるだけで品物の見分けが付かない．いくら訓練を積んでも男女の区別は難しいばかりか, 二人の息子の見分けすらできない．要するに人は，ニューロン網の構築によって，見たいように見ているのである．認識とは何かを考えるには実に良い本だと思う．

閑話休題．本題に戻って同値関係の 3 条件は独立であろうか．たとえば推

移律が対称律と反射律から証明されることはないであろうか．これを確かめるには一つの公理が成り立たず，残りの公理は満たされているような関係の実例を作ればよい．

例　$\mathbb{R}$ において

$$a \sim b \iff |b-a| \leqq 1$$

と定義すれば条件 1, 2 は成立するが条件 3 は成立しない．$a=1, b=2, c=3$ はその例である．したがって，条件 3 は条件 1, 2 から独立である．

例　$\mathbb{R}$ において

$$a \sim b \iff a \leqq b$$

と定義すれば条件 1, 条件 3 は成立するが，条件 2 は満たされない．したがって，条件 2 は条件 1，条件 3 と独立である．

問題　条件 2，3 は満たされるが，条件 1 は満たされない実例を作れ．

この問題はちょっと正解を得にくい．試行錯誤的に作ってもなかなかうまくいかない．なぜなら条件 1 が一見条件 2, 3 から証明されるように見えるからである．この証明の誤りに気が付けばそこから実例作りの糸口が得られる．

集合 S において関係 $\sim$ は条件 2，条件 3 を満たすとする．

$$a \sim b \text{ より } b \sim a \quad \text{by } 2,$$
$$a \sim b,\ b \sim a \Longrightarrow a \sim a \quad \text{by } 3.$$
$$\therefore \quad a \sim a$$

この証明らしきものの誤りは $a \sim b$ となる b が存在するとは限らぬところにある．すなわち $a \sim b$ が満たされなければ $b \sim a$ とは結論できない．したがって，逆に言えば，a に対して $\exists b(\in S)[a \sim b]$ ならば上の証明が通用して

$a \sim a$ が成り立つことになる．つまり条件 1 は

1′.　$\forall a(\in S)\exists b(\in S)[a \sim b]$

と置き換えられるわけである．

上の問題を講義中に出したら，次のような鮮やかな解答が返って来た：$\mathbb{R}$ において

$$a \sim b \Longleftrightarrow ab \neq 0$$

と定義すると $0 \sim 0$ は成り立たない．条件 2, 3 は明らかに成り立つ．0 には自分も含めて相部屋のものがいないのだ．とにかく，上の証明の誤りの指摘もせぬ内にサッと解答が出たのには驚いた．できたら 1 万円やる，なんて見得を切らなくてよかった．

§ 2. 「等しい」ということの考察

前節で類別という言葉に関連して，色々述べた．同値関係とは三つの条件 (反射律，対称律，推移律) を満たす関係のことだが，これは同値関係が等号 (=) に近い性質を持っているということを示すもので，等号はそれ自身が同値律を満足することは言うまでもない：

1. (反射律)　$x = x$
2. (対称律)　$x = y \Longrightarrow y = x$
3. (推移律)　$x = y,\ y = z \Longrightarrow x = z$

ところで，この = は何が「等しい」ということを意味するのだろうか，読者は考えてみたことがおありだろうか．= は「どこからどうみてもまったく同じものである」ということを意味しているのではない．

たとえば $1 + 1 = 2$ を例にして考えてみよう．両辺は「どこからどうみてもまったく同じもの」だとは言えない．両辺の表す個数が同じものだと見るか，両辺の表す集合が等しいと見るか，あるいはそれ以外のどういう見方であろうと，まったく同じものではないからこそ，そういう「同じとみなす見方」が必要となるのである．

もう一つ例を挙げよう．$0.999\cdots = 1$ はおかしいと文句を付ける人が結構

多い．中には，市販とはいえ学術的な雑誌にこうしたことを書いている哲学の人がいたのには驚いた．$0.999\cdots = 1$ は収束の「定義」に基づく結果なのであって，間違っているとか，おかしいとかいうような筋合いのものではない．見た目の形が異なることは誰の目にも明らかであるから「どこからどうみても同一のもの」であるはずがないではないか．

そもそも，$x = y$ とせよ，という表現すら，等号が「同一物」しか表さないのだとすると，「おかしい」．x は x であり，y は y であるからだ．

結局，こうした例を見ていくと「等号」(=) とは，対象のある性質に注目して，その同じ性質を持っているときに「等しい」とみなしている (定義している) のだということが判るだろう．

そうすると，等号もまた同値類別に外ならないことになる．しかし，その学問分野の基本にかかわるような類別にまで $\sim$ とか $\equiv$ といった記号を使うわけにはいかない．たとえば，集合論において集合 x, y が等しい ($x = y$) とは，結局のところ，単に $=$ が同値律を満たすというにとどまらず，どのような論理式においても，x が現れたなら，それを y に置き換えられる，そういう意味で，その分野では「同じもの」であると認める，ということであろう．

そのように置き換えてよいことをどうやって証明するのだろうか？　個々の場合にはその等しさの吟味によって置換の可能性を論じることはできるかもしれないが，任意の論理式に対して x を y に置き換えてよいことは「公理として」認める以外にはないのではなかろうか．その公理は，数学 (端的に言えば，すべての数学の基盤である集合論) を始める前の，数学の文法 (言語) を定める段階で提示するのが普通である．

つまり，次のことを数学言語 (われわれは**述語論理**を使う) の中で公理として認めるのである：

等号公理

1. (**反射律**)　$x = x$
2. (**代入法則**)　$\varphi(x)$ を x に関する命題で y を含まないものとするとき，

$$x = y \wedge \varphi(x) \Longrightarrow \varphi(y)$$

反射律は「同じものは等しい」という意味内容である．代入法則は「二つの対象が等しいならば，一方が φ という性質を持つとき，他方も φ という性質を持つ」という意味である．

代入法則から，対称律 $(a = b \Rightarrow b = a)$，推移律 $(a = b,\ b = c \Rightarrow a = c)$ は $\varphi(x)$ をそれぞれ $x = a$，あるいは $a = x$ と置けば簡単に導出される (読者自身試みよ)．

ところで，われわれ数学者には，集合 a，b について

$$(a \subseteqq b) \wedge (b \subseteqq a)$$

をもって $a = b$ の定義だと思っている者が多い．しかし，これが等号の定義なら，この $a = b$ の定義から

$$a \in X \Longleftrightarrow b \in Y$$

はどうやって証明するのだろうか？　これはできぬ相談である．なぜなら，構成要素が一致することをもって相等の定義がされているだけなのだから．

だから，集合論では外延性公理として

$$(a \subseteqq b) \wedge (b \subseteqq a) \Longrightarrow a = b$$

を採用するが，普通は逆向きの $\Leftarrow$ は書かれていない．逆向きは等号公理から必然的に従うのである．

もしも等号公理を言語 (論理) の方の公理として採用するのでなければ，$a = b$ の定義を

$$(a \subseteqq b) \wedge (b \subseteqq a) \text{ かつ } (a \in X \Longleftrightarrow b \in Y)$$

とせねばならない．

§ 3. イデアル

R を環とする．われわれの場合環とは単位元を有する可換環のことである．

定義　R の部分集合 A $(\neq \varnothing)$ が R の**イデアル**であるとは，

1. A は R の加法で群をなす．
2. $a \in A,\ r \in R$ に対して $ra \in A$.

の2条件が満たされるときに言う．

R 自身および $\{0\}$ は R のイデアルである．また $a \in R$ のとき，

$$(a) = \{xa \mid x \in R\}$$

は R のイデアルをなす．これを a から生成される**単項イデアル**と言う．

問題　(a) がイデアルをなすことを示せ．

1を R の乗法単位元とすると $(1) = R$，また $(0) = \{0\}$ であるから $R, \{0\}$ は単項イデアルの一種である．

さらに一般に $a_1, \cdots, a_n \in R$ のとき

$$(a_1, \cdots, a_n) = \left\{ \sum_{j=1}^{n} x_j a_j \,\middle|\, x_j \in R\ (j = 1, \cdots, n) \right\}$$

とすると，$(a_1, \cdots, a_n)$ は R のイデアルであることが容易に知られる．これを $a_1, \cdots, a_n$ から生成されるイデアルと言う．$(a_1, \cdots, a_n)$ は $a_1, \cdots, a_n$ を含む最小のイデアルである．

例　$R = \mathbb{R}[X, Y]$，すなわち2変数 X, Y の実数係数多項式全体のなす環（$\mathbb{R}$ 上の2変数多項式環と言う）を考える．

イデアル $(X-1)$ は $X-1$ で割り切れるような X, Y の多項式全体の集合である．また

$$(X, Y) = \{f(X,Y)X + g(X,Y)Y \mid f(X,Y), g(X,Y) \in \mathbb{R}[X,Y]\}$$

は定数項が0の多項式全体のなす集合である．

R が $\mathbb{Z}$ であるとき (a,b) は最大公約数の記号と混同しそうだが，意図的にそうしているのである．混同して良い理由はすぐにわかる (定理 3.2).

例題　$R=\mathbb{Z}$ とする．$(6,4)=(2)$ である．

証明　$6 \in (2)$ だからイデアルの性質 2 によって $x \in \mathbb{Z}$ に対して $6x \in (2)$. 同様に $4 \in (2)$ だから $4y \in (2)(\forall y \in \mathbb{Z})$. イデアルの性質 1 によって

$$6x+4y \in (2) \quad (\forall x \forall y \in \mathbb{Z})$$

$$\therefore \quad (6,4) \subseteqq (2)$$

逆に $2 = 6 \cdot 1 + 4(-1) \in (6,4)$ だから

$$(2) \subseteqq (6,4) \quad \therefore \quad (6,4)=(2) \quad \|$$

次の定理は重要である．

定理 3.1　有理整数環 $\mathbb{Z}$ は**単項イデアル環**である (すなわち，$\mathbb{Z}$ のイデアルはすべて単項イデアルである).

証明　A を $\mathbb{Z}$ のイデアルとする．$A=(a)$ となる $a \in \mathbb{Z}$ の存在することを証明する．$A=\{0\}$ ならば $A=(0)$ だから問題ない．そこで $A \neq 0$ とする．$a \in A$ のうち $|a|$ が最小正のものを取る：$0<|a| \leqq |b|$ $(\forall b \in A)$.

$b \in A$ とする．割算の原理 (定理 1.1) により

$$b = qa + r, \qquad 0 \leqq r < |a|$$

を満たす $q, r(\in \mathbb{Z})$ が存在する．

$$r = b + (-q)a \in A$$

なぜなら $a \in A$ より $(-q)a \in A$，また $b \in A$ より $r = b+(-q)a \in A$. 一方 $r<|a|$ であり，a は A の元で $|a|$ は最小正だから $r=0$ でなくてはならない．

$$\therefore \quad b = qa \in (a) \quad \therefore \quad A=(a) \quad \|$$

定理 3.2　$a_1, \cdots, a_n \in \mathbb{Z}$ とし，$a_1, \cdots, a_n$ の最大公約数を d とすると

$$(a_1, \cdots, a_n) = (d)$$

証明　定理 3.1 によって

$$(a_1, \cdots, a_n) = (b)$$

なる $b \in \mathbb{Z}$ が取れる．

$$a_j \in (b) \quad \therefore\ a_j \equiv 0 \pmod{b} \quad (j = 1, \cdots, n)$$

故に b は $a_1, \cdots, a_n$ の公約数．$\therefore\ b|d$

逆に，$b \in (a_1, \cdots, a_n)$ だから $\exists x_1, \cdots, x_n (\in \mathbb{Z})$；

$$a_1x_1 + \cdots + a_nx_n = b$$

しかるに $a_j = db_j$ $(j = 1, 2, \cdots, n)$ と表せるから

$$d(b_1x_1 + \cdots + b_nx_n) = b \quad \therefore \quad d|b \quad \therefore \quad b = \pm d \quad \|$$

定理 3.2 によって最大公約数の記号をイデアルに流用した理由が納得されたであろう．

問題　$\mathbb{Z}$ において次を示せ：

$$a|b \Longleftrightarrow b \in (a) \Longleftrightarrow (b) \subseteqq (a)$$

特に a, b が互いに素な整数であるためには

$$(a, b) = \mathbb{Z}$$

が必要十分である．$(1) = \mathbb{Z}$ に注意すると「互いに素」を数の場合と同じく $(a, b) = 1$ と表しても混乱は生じない．

系　$a_1, \cdots, a_n$ および b を整数とする．不定方程式

$$a_1x_1 + \cdots + a_nx_n = b \tag{2}$$

が整数解を持つためには

$$(a_1, \cdots, a_n)|b$$

が必要十分である．

証明　$d=(a_1,\cdots,a_n)$ とすると，イデアルとして

$$(a_1,\cdots,a_n)=(d)$$

方程式 (2) が解を有するとは $b\in(a_1,\cdots,a_n)$ のことだから，$b\in(d)$，すなわち $d|b$ が条件である．∥

(2) の整数解を求めるために，$a_1,\cdots,a_n$ の 1 次結合として表せる整数の全体 $(a_1,\cdots,a_n)$ を考えたところに一種の発想の逆転がある．その鮮やかさに注目しよう．

単項イデアル環というのはいろんな意味で重要であるが，果たしてどういう条件が満たされれば単項イデアル環になるであろうか．

有理整数環 $\mathbb{Z}$ が単項イデアル環であることが証明できた経過をたどってみればわかるように，$\mathbb{Z}$ では割算の原理が成り立つことが基本的役割を果している．そこで思い出すのは多項式も割算ができることだ．

$\mathbb{R}[X]$ を実数係数で変数 X の多項式全体のなす環とする ($\mathbb{R}$ 上の 1 変数多項式環)．$f(X)\in\mathbb{R}[X]$ の次数を $\deg f$ と記す．特に，定数 $c\ (\neq 0)$ に対しては $\deg c=0$ である．$\deg 0$ は定義しない．

定理 3.3 (多項式の割算の原理)　$f(X)(\neq 0), g(X)\in\mathbb{R}[X]$ とする．

$$g(X)=q(X)f(X)+r(X),\quad (r=0)\vee(\deg r<\deg f)$$

を満足する $q(X), r(X)(\in\mathbb{R}[X])$ が存在する．

この定理は既知としよう．実際自分で証明されるとよい．この割算の原理のおかげで，1 変数多項式環 $\mathbb{R}[X]$ は $\mathbb{Z}$ に酷似した性質を有することになるのである．たとえば

定理 3.4　$\mathbb{R}[X]$ は単項イデアル環である．

証明は各自試みよ．

[ヒント]　定理 3.1 の証明において $|a|$ のかわりの $\deg f$ を使う．すなわち次数最小の多項式 f を選び，他の多項式はすべて $h(X)f(X)$ と書けることを示せばよい．

定理 3.5　$f_1, \cdots, f_n \in \mathbb{R}[X]$ とし，$f_1, \cdots, f_n$ の最大公約多項式を d とすると

$$(f_1, \cdots, f_n) = (d).$$

系　$f(X), g(X) \in \mathbb{R}[X]$ とする．

$$(f, g) = 1 \Longleftrightarrow \exists p \ \exists q \ (\in \mathbb{R}[X]) \ [pf + qg = 1]$$

この系は次のように微積分学で暗黙裏に使われている：

問題　$f, g \in \mathbb{R}[X]$ とし，$f = f_1 \cdot f_2$，$f_1, f_2 \in \mathbb{R}[X]$，しかも $(f_1, f_2) = 1$ とする．すると $\dfrac{g}{f}$ は

$$\frac{g}{f} = \frac{g_1}{f_1} + \frac{g_2}{f_2} \quad (g_1, g_2 \in \mathbb{R}[X])$$

と分解 (部分分数分解) される．

有理関数の積分は分母が $(x^2 + a^2)^n$ のものと $(x + a)^n$ のものとに分けられるというアレである．証明は系から直ちに得られるから読者に任せる．

これらの証明をたどってみることは数学のある面を理解するのに役立つであろう．すなわち形の上の類似が本質的なのだということである．多項式環 $\mathbb{R}[X]$ と有理整数環 $\mathbb{Z}$ とでは中味から言うと同じようなものとはとても言えないのに，実際は驚くほど共通点を持っている．$\mathbb{Z}$ と酷似しているのは，$\mathbb{Z}[X]$ であろうと思っても不思議はないが実はそうではない．実際，$f(X) = 2X$，$g(X) = X^2$ とすればわかるように $\mathbb{Z}[X]$ では定理 3.3 が成り立たないから

だ．その原因は $\mathbb{Z}$ では割算が自由にできないことに帰せられる．以上の議論から $\mathbb{C}[X], \mathbb{Q}[X]$($\mathbb{C}, \mathbb{Q}$ はそれぞれ複素数体，有理数体を表す) においても割算の原理が成り立つことが理解されよう．

定義　単位元 e を持つ環 R は条件

$$\forall x(\neq 0)\exists y(\in R);\ xy = yx = e$$

を満たすとき，すなわち $R^\times = \{x\ (\in R) \mid x \neq 0\}$ が乗法に関して群をなすとき，言い換えれば割算が自由にできるとき，**体** (field) と呼ばれる．

ドイツ語では Körper，フランス語では corps という．これらは共に「身体」という意味である．なんとなくその気持がわかるような気もする．一方，field には身体という意味はない．作業をする「場」という意味なのだろう．

この奇妙な用語の起源について一言．ヴェーバー (1842–1913) が類体に関連して使ったのを受けて，一般に代数体の意味でデデキントが使い始めた．抽象的な体の意味ではシュタイニッツが最初であろう．英語ではなかなか用語が定まらず 1930 年代に field が使われ始めた．

$\mathbb{C}, \mathbb{R}, \mathbb{Q}$ は体である (それぞれ，**複素数体**，**実数体**，**有理数体**と呼ばれている) が，$\mathbb{Z}, \mathbb{C}[X], \mathbb{C}[X, Y]$ 等は体ではない．また p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ は体である．なぜなら $\overline{0}$ 以外の剰余類の集合 $(\mathbb{Z}/p\mathbb{Z})^\times$ は乗法で群をなすからである．しかるに m が合成数であれば $\mathbb{Z}/m\mathbb{Z}$ は体ではない．たとえば $m = m_1m_2\ (m_1 \neq 1, m_2 \neq 1)$ とすると

$$\overline{m_1} \neq 0, \quad \overline{m_2} \neq 0 \quad \text{but} \quad \overline{m_1} \cdot \overline{m_2} = \overline{m_1m_2} = \overline{0}$$

だから零元でないものの積が零元となる．これでは逆元を持ち得ない．($\because$ $\overline{m_1}$ が逆元 $\overline{a}$ を持つとすると $\overline{m_2} = \overline{1} \cdot \overline{m_2} = (\overline{a} \cdot \overline{m_1})\overline{m_2} = \overline{a}(\overline{m_1} \cdot \overline{m_2}) = \overline{a} \cdot \overline{0} = \overline{0} \quad \therefore\ \overline{m_2} = \overline{0}$ となり矛盾) こんな事情があるから $\overline{0}$ ばかりでなく m と素でない類を全部取除いて $(\mathbb{Z}/m\mathbb{Z})^\times$ を作り，群にしたのだった．

$\mathbb{Z}/p\mathbb{Z}$ は有限体の代表で，しばしば $\mathbb{F}_p$ と記される．

定理 3.6　F を体とすると $F[X]$ では割算の原理が成り立つ．すなわち $f, g \in F[X]$ とすると $f \neq 0$ のとき，

$$g = qf + r, \quad (\deg r < \deg f) \vee (r = 0)$$

なる $q, r \in F[X]$ が存在する．

[注意]　$F[X]$ は F の元を係数，X を変数とする多項式全体のなす環で，F 上の 1 **変数多項式環**と呼ばれる．二つの多項式は係数が F の元として等しいとき，相等しいと定義する．また $f(X) = a_0 X^n + \cdots + a_n$ $(a_0 \neq 0)$ のとき $\deg f = n$ と定義する．たとえば $f = pX^2 + X$ は $\mathbb{R}[X]$ では $\deg f = 2$ だが，$\mathbb{F}_p[X]$ の多項式とみると $f = X$ で $\deg f = 1$ である．

系　F を体とすると $F[X]$ は単項イデアル環である．

問題　(因数定理)　$f(X) \in F[X]$ とする．$f(X)$ が $X - \alpha$ $(\alpha \in F)$ で割り切れるためには $f(\alpha) = 0$ が必要十分である．

問題　$\alpha_1, \cdots, \alpha_n$ を F の相異なる元とする．$f(\alpha_1) = 0, \cdots, f(\alpha_n) = 0$ ならば $f(X)$ は $(X - \alpha_1) \cdots (X - \alpha_n)$ で割り切れる．

[ヒント]　$f(\alpha_1) = 0$ より $f(X) = (X - \alpha_1) f_1(X), f_1(X) \in F[X]$ と表せる．

問題　$f(X) \in F[X], \deg f = n$ とすると $f(X)$ は F 内では高々 n 個の零点しか持ち得ない．

最後の問題を $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ の場合にあてはめると，次を得る：

定理 3.7　p を素数とし $f(X) \in \mathbb{Z}[X]$ とすると，

$$f(X) \equiv 0 \pmod{p}$$

は p を法として高々 $\deg f$ 個しか整数解を持ち得ない．

上の問題から $F[X]$ というのは $\mathbb{R}[X]$ と全く同様に，もとに戻って言えば F は $\mathbb{R}$ や $\mathbb{Q}$ と同様に取り扱えることがわかる．これが抽象数学の威力なのだが，その面白さも何か身近な，いわゆる具体的な問題に応用されないと本当に面白いとは思えぬのが人情というものである．そこで一つ：

定理 3.8 (ウィルソンの定理)　p を素数とすると

$$(p-1)! \equiv -1 \pmod p$$

証明　体 $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ と書く．$\mathbb{F}_p[X]$ の多項式

$$f(X) = X^{p-1} - 1$$

を考える．フェルマーの小定理によって $f(1) = f(2) = \cdots = f(p-1) = 0$ が成り立つ．ここにおける $0, 1, \cdots$ 等は $\mathbb{F}_p$ において考えているのだし，等号も $\mathbb{F}_p$ において考えているのである．$\mathbb{F}_p$ においても $1, 2, \cdots, p-1$ は相異なるから，上記の問題から $f(X)$ は $\mathbb{F}_p[X]$ の多項式として $(X-1)(X-2)\cdots(X-p+1)$ で割り切れる．次数と最高次の係数を比較して

$$f(X) = (X-1)(X-2)\cdots(X-p+1)$$

を得る．定数項の比較によって

$$(p-1)! = -1 \quad \text{in } \mathbb{F}_p \qquad \therefore \quad (p-1)! \equiv -1 \pmod p \quad \|$$

なお，同時に $\sum_{i<j} i \cdot j \equiv 0 \pmod p$ 等も知られる．

ウィルソンの定理のおもしろいのは逆も成り立つところである．すなわち

$$(q-1)! \equiv -1 \pmod q \quad \Longrightarrow \quad q \text{ は素数}$$

である．証明は簡単だから読者にお任せする．

どんな環でもみな単項イデアル環だと思われても困るから単項イデアル環でない例を挙げておこう．

例　2 変数多項式環 $\mathbb{R}[X, Y]$ のイデアル (X, Y) は単項イデアルではない．故に $\mathbb{R}[X, Y]$ は単項イデアル環ではない．

証明は $(X,Y)=(f)$ となる $f\in\mathbb{R}[X,Y]$ が存在するという仮定から矛盾を導けばよい．

うっかり書き漏らしそうになったが，$\mathbb{Z}$ や $\mathbb{R}[X]$ における割算の原理の重要なもう一つの側面を述べておく．どちらでも同じだから $\mathbb{R}[X]$ の方で述べる．

$$g=qf+r,\quad (\deg r<\deg f)\vee(r=0)$$

のとき，

$$(g,f)=(f,r)$$

が成立する．なぜなら $h|g$ かつ $h|f$ ならば $r=g-qf$ より $h|r$．逆に $h|f$ かつ $h|r$ ならば $g=qf+r$ により $h|g$ だからである．これによって整数の場合同様，f と g の最大公約多項式を求めるアルゴリズム (**ユークリッドのアルゴリズム**) が得られる．

例題　$\mathbb{R}[X]$ で $f=2x^4+2x^3+3x^2+x+1$ と $g=x^4+x^3-x^2-2x-2$ の最大公約式を求めよ．

解答

$$g=\frac{1}{2}\cdot f-\frac{5}{2}(x^2+x+1),$$

$$\therefore\ (g,f)=(f,\frac{5}{2}(x^2+x+1))=(f,x^2+x+1)$$

f を x^2+x+1 で割ると割り切れて (つまり，余り 0)，

$$f=(2x^2+1)(x^2+x+1)$$

$$\therefore\quad (f,g)=(x^2+x+1,0)=x^2+x+1$$

問題　$x^5-3x^2+2x^2-6$ と $x^7+2x^4+3x^3+6$ の最大公約式を求めよ．

問題　$(2873,6137)$ を求めよ．

［ヒント］　$\mathbb{Z}$ でのユークリッドのアルゴリズムを用いること．

与えられた自然数 q が巨大なとき，q が素数であることを判定するのはとても困難なことであるのに，公約数を求めるのは，どんなに大きな 2 数に対しても，上の方式で容易に求まるのは不思議なことである．

第4章　演算の遺伝

§1. 演算の遺伝

G を群とする．$\sim$ を G における同値関係とする．すなわち，

1. (反射律)　$a \sim a$
2. (対称律)　$a \sim b \Longrightarrow b \sim a$
3. (推移律)　$a \sim b, b \sim c \Longrightarrow a \sim c$

が満たされるとする．$\overline{a}$ でもって a と同値な元の集合を表すことにする：

$$\overline{a} = \{x\ (\in G) \mid x \sim a\}$$

このような同値類 $\overline{a}$ を一つの要素に見立てて，それら全体の集合を $\overline{G}$ とか $G/\sim$ とかで表すことにする．

$\overline{G}$ の 2 元 $\overline{a}, \overline{b}$ に対して積 $\overline{a} \cdot \overline{b}$ を

$$\overline{a} \cdot \overline{b} = \overline{ab} \tag{1}$$

によって定義するとき，この演算のもとで $\overline{G}$ が群をなすのはどんなときであろうか．この問題を考えてみよう．

定理 4.1　(1) によって $\overline{G}$ に演算を導入するとき，$\overline{G}$ が群をなす必要十分条件は同値関係 $\sim$ がさらに条件

$$a \sim a',\ b \sim b' \Longrightarrow ab \sim a'b' \tag{2}$$

を満たすことである．

証明　$\overline{G}$ が群をなすとすれば，$a \sim a', b \sim b'$ のとき $\overline{a} = \overline{a'}, \overline{b} = \overline{b'}$ であるから $\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$ でなくてはならない．定義 (1) より $\overline{ab} = \overline{a'b'}$ $\quad\therefore\ ab \sim a'b'$ となり (2) が成り立つ．逆に (2) が成り立つとしよう．(1) によって演算を定義すれば (2) のおかげで演算の結果が代表元の取り方に関係しないことがわかり (1) がいわゆる well defined (合理的に定義されている) であることが言えた．$\overline{G}$ の単位元は $\overline{e}$ で，$\overline{a}$ の逆元は $\overline{a^{-1}}$ であることは (1) を用いてたちまち証明されるから演習問題ということにしよう．‖

集合を元 (要素) として演算を定義するとき，上の well defined という概念は大切である．初心者はよく見落とすので特に注意せねばならない．たとえば組織間の協定を結ぶおり，代表者が変われば協定の内容も変わるのが世間では常識だろうが数学ではそれは困る．集合を元，すなわち最小単位とする意味がなくなるから．

さて，(2) を満たすような同値関係 $\sim$ があるとして，

$$N = \{x(\in G) \mid x \sim e \text{ (単位元)}\} \, (= \overline{e})$$

と置く．すると N は G の部分群をなす．実際，$x \in N, y \in N$ ならば (2) により $xy \sim e^2\ (= e)$ $\quad\therefore\ xy \in N$．また $x \in N$ ならば

$$x \sim e,\ x^{-1} \sim x^{-1}$$

だから (2) のおかげで

$$xx^{-1} \sim ex^{-1} \quad \therefore\ \ e \sim x^{-1} \quad \therefore\ \ x^{-1} \in N$$

を得るからである．

また $a \in G, b \in G$ に対して

$$a \sim b \Longleftrightarrow ba^{-1} \in N \ (\Longleftrightarrow b \in Na) \tag{3}$$

が成り立つ．これは $a \sim b, a^{-1} \sim a^{-1}$ より $ba^{-1} \in N$ が得られるし，$ba^{-1} \in N$ ならば $ba^{-1} \sim e$ より $b \sim a$ が得られるからである．

さらにそれだけではない．$x \in N$ とすると N の定義から $x \sim e$.

$$\therefore\ \ axa^{-1} \sim aa^{-1} = e \ (\forall a \in G)$$

すなわち

$$axa^{-1} \in N \ (\forall a \in G, \forall x \in N) \tag{4}$$

そこで $aNa^{-1} = \{axa^{-1} \mid x \in N\}$ と記せば (4) は

$$aNa^{-1} \subseteqq N \quad (\forall a \in G) \tag{5}$$

とも書ける．

定義 群 G の部分群 N が (5) を満たすとき N は G の**正規部分群** (normal subgroup) であると言われる．

以上で $\overline{G}$ が群をなすような同値関係 $\sim$ があれば単位元と同値な元の全体 N は G の正規部分群をなし，(3) という重要な関係で $\sim$ と N とは結びつけられていることがわかったのである．

逆に N が G の正規部分群であれば関係 $\sim$ を (3) によって定義すれば $\sim$ は同値関係となることは簡単にわかる．そこで $a \in G$ に対し $\overline{a} = \{x \ (\in G) \mid x \sim a\}$ とおいて (1) によって演算を定義すれば $\overline{G}$ は群をなす．これを示すには定理 4.1 によって (2) が成立することを次のように確かめればよい．

$a \sim a', b \sim b'$ とする．(3) によって

$$\exists x \ \exists y (\in N) \ [xa = a', \ yb = b']$$
$$\therefore \quad a'b' = (xa)(yb) = x(aya^{-1})ab$$

N は正規だから $aya^{-1} \in N \quad \therefore \ x(aya^{-1}) \in N \quad \therefore \ a'b' \sim ab$

演算を剰余類に遺伝するような同値関係と正規部分群とは (3) を仲介として 1 対 1 に対応していることが解明されたのである．$\overline{G}$ を G/N とも記し，G の N による**剰余類群**とか**商群**とかいう．

問題 (5) は

$$aNa^{-1} = N \ (\forall a \in G)$$

とも，また

$$aN = Na \ (\forall a \in G)$$

とも同値である．

問題　G がアーベル群であれば，すべての部分群は正規である．

これまでの考察を環で行なうとどうなるであろうか．つまり，環の 2 演算 $+, \cdot$ が遺伝するのは $\sim$ がどんな条件を満たすときであろうか．また正規部分群に対応する概念は？　その解答は次の通り：

定理 4.2　R を (単位元を有する可換) 環とする．また $\sim$ を R における同値関係とする．同値類の集合 $\overline{R}$ に加法・乗法を

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

で定義するとき，$\overline{R}$ が再び環となるためには $a \sim a', b \sim b'$ ならば

$$a + b \sim a' + b', \quad ab \sim a'b' \tag{6}$$

が満たされることが必要十分である．

しかもこのとき，$A = \{x(\in R) \mid x \sim 0\}$ と置けば，A は R のイデアルをなす．逆に A が R のイデアルをなすならば $a, b(\in R)$ に対して

$$a \sim b \Longleftrightarrow a - b \in A$$

によって $\sim$ を定義すると $\sim$ は (6) を満足する同値関係である．$\overline{R}$ は**剰余環**とか**商環**とか呼ばれる．

問題　定理 4.2 を証明せよ．

$m \in \mathbb{Z}$ のとき $(m) = m\mathbb{Z}$ は $\mathbb{Z}$ のイデアルである．だから $\mathbb{Z}/m\mathbb{Z}$ は環となるのだということが理解される．もしも環 R がさらに体であればイデアルより強いどんな概念に発展するのだろう，と考えてみるのは良いが，実は何にもならない．というのは，次が成り立つからである：

問題　体 F のイデアルは F 自身と $\{0\}$ 以外に存在しないことを示せ．

第 3 章とあわせて考えるとイデアルには二つの起源があることがわかる．すなわち部分集合から生成される 1 次結合の全体という考え方と，もう一つは類別における加法単位類という考え方がそれである．歴史的に見れば，前者の方が先に登場した．次に後者の方の応用について述べることにしよう．

§ 2. 剰余環の考え方の応用

§ 2.1　実数体の構成

$\mathbb{Q}$ を有理数体とする．有理数は rational number だから $\mathbb{R}$ と書きたい所なのだが実数 (real number) がやっぱり R で始まって具合が悪いから R の手前で $\mathbb{Q}$ にするのだ．($\mathbb{C}$ は複素数 complex number の C である．$\mathbb{Z}$ はドイツ語の整数 ganze Zahl の Z を使ったものである．) なお，rational は ratio (比) を語源として持つから本当は有比数 (整数の比で表せる数) と訳すべきだったと言われている．もっともだと思う．無理な数とはひどい，無理数に気の毒だとは思うが今さらどうしようもない．

徒し事(あだしごと)はさておき，$\mathbb{Q}$ から $\mathbb{R}$ を構成するカントルの方法を説明しよう．

数列 $\{a_n\}(a_n \in \mathbb{Q})$ が $a \in \mathbb{Q}$ に収束するとは

$$\forall\varepsilon(>0)\exists N; |a-a_n|<\varepsilon\ (\forall n \geqq N)$$

が成り立つことであった．$\{a_n\}$ が a に収束するならば

$$\forall\varepsilon(>0)\exists N; |a_m-a_n|<\varepsilon\ (\forall m\forall n \geqq N) \tag{7}$$

が成り立つ．しかし逆に (7) が成り立つからといって有理数列 $\{a_n\}$ が $\mathbb{Q}$ の数に収束するとは限らない．たとえば $\sqrt{2}$ の小数点以下第 n 桁まで取った有限小数を a_n とすれば $\{a_n\}$ は (7) を満たすが $\mathbb{Q}$ の数には収束しない．つまり $\mathbb{Q}$ には目には見えぬが，穴があいている．そこでどうするかというと (7) を満たすような数列自身を一つの数とみなすのである．$\sqrt{2}$ に収束する数列を $\sqrt{2}$ とみなすのだ．有理数に収束するような数列はその有理数と同一視す

る．こうすれば穴のあいていない数の集合ができあがるだろう $\cdots$ とカントルは考えた，かどうかは保証できないが，正確に言えば次のようになる．

定義 (7) を満たす $\mathbb{Q}$ の数列は**基本列**と呼ばれる．

基本列というのはカントルの命名である．**コーシー列**とも呼ばれるが，フランス人は何でもコーシーが既に考えていたことにしたがるから，これはフランス流の呼び名だろうと思われる．

$\mathbb{Q}$ の基本列のなす集合を $\mathfrak{R}$ と書く ($\mathfrak{R}$ は R のドイツ文字)．$\mathfrak{N}$ でもって 0 に収束する基本列のなす集合とする ($\mathfrak{N}$ は N のドイツ文字)．しからば容易にわかるように $\mathfrak{R}$ は数列の和・積の演算で環をなし，$\mathfrak{N}$ はそのイデアルである．$\mathfrak{R}/\mathfrak{N}$ を $\mathbb{R}$ と記す．$a_n = a(\forall n \in N)$ なる数列を有理数 a と同一視する．そして写像

$$\varphi : \mathbb{Q} \longrightarrow \mathbb{R}$$

を

$$\varphi(a) = \overline{a} = \{a\} \bmod \mathfrak{N}$$

で定義する．ここに $\{a\}$ は $a_n = a\ (n \in \mathbb{N})$ なる数列である．

問題　この φ は単射で，しかも準同型写像である：

$$\varphi(a+b) = \varphi(a) + \varphi(b),\ \varphi(ab) = \varphi(a)\varphi(b)$$

この問題の意味するところは $\mathbb{Q}$ と $\varphi(\mathbb{Q})$ とは加法と乗法という演算に注目するかぎりでは同一の構造を持っているということだから $\varphi(a)$，すなわち，有理数 a に収束する数列の全体にまた a という文字を割り当てることにしよう．

基本列 $\alpha = \{a_n\}$ が $\alpha \notin \mathfrak{N}$ ならば，すなわち $\overline{\alpha} \neq \overline{0}$ ならば $\left\{\dfrac{1}{a_n}\right\}$ なる数体も基本列となり，それを β とすると，$\overline{\alpha} \cdot \overline{\beta} = \overline{1}$ となる．すなわち環 $\mathbb{R}$ は

体となる．

次に $\mathbb{R}$ において順序 $x<y$ と絶対値 $|x|$ を次のように定義する．

$\alpha \in \mathbb{R}$ のとき α はある有理数列 $\{a_n\}$ の類 $(\alpha = \{a_n\} + \mathfrak{N})$ なのだが，この類を $[a_n]$ と記そう：$\alpha = \{a_n\} + \mathfrak{N} = [a_n]$

$$\alpha \geqq 0 \Longleftrightarrow \exists N; a_n \geqq 0 \ (\forall n \geqq N)$$
$$\alpha \leqq 0 \Longleftrightarrow \exists N; a_n \leqq 0 \ (\forall n \geqq N)$$
$$\alpha \geqq \beta \Longleftrightarrow \alpha - \beta \geqq 0$$
$$\alpha > \beta \Longleftrightarrow \alpha \geqq \beta \quad \text{かつ} \quad \alpha \neq \beta$$

また

$$|\alpha| = \begin{cases} \alpha & (\alpha \geqq 0 \text{ のとき}) \\ -\alpha & (\alpha \leqq 0 \text{ のとき}) \end{cases}$$

不等号 $\leqq$ や絶対値 $|\ |$ が定義されれば，収束や基本列の定義は簡単である．

$\mathbb{R}$ の数列 $\{\alpha_n\}$ が $\alpha \in \mathbb{R}$ に収束する $(\alpha = \lim_{n\to\infty} \alpha_n)$ とは

$$\forall \varepsilon (>0)\ \exists N (\in \mathbb{N}) \forall n (\geqq N)\ [|\alpha - \alpha_n| < \varepsilon]$$

が成り立つことであり，$\{\alpha_n\}$ が基本列であるとは

$$\forall \varepsilon (>0) \exists N (\in \mathbb{N}) \forall m \forall n (\geqq N) [|\alpha_m - \alpha_n| < \varepsilon]$$

が成り立つことである．このとき次が眼目の結果である：

定理 4.3 (完備性)　$\mathbb{R}$ の基本列は $\mathbb{R}$ の元に収束する：

$$\{\alpha_n\} : \text{基本列} \Longrightarrow \lim_{n\to\infty} \alpha_n \in \mathbb{R}$$

証明 (証明の概略)　1. $\alpha \in \mathbb{R}$ を $\alpha = [a_n]$ $(a_n \in \mathbb{Q})$ と表す．$a_n \in \mathbb{R}$ と見たときの数列 $\{a_n\}$ が α に収束すること，つまり $\lim_{n\to\infty} a_n = \alpha$ であることは $|\alpha - a_n| \leqq \varepsilon$ は，ある N に対して $|a_m - a_n| \leqq \varepsilon \quad \forall m \forall n\ (\geqq N)$ が成り立つこととして定義されていることから明らかである．

2. $\{\alpha_n\}$ $(\alpha_n \in \mathbb{R})$ が基本列であるとして $\lim_{n\to\infty} \alpha_n \in \mathbb{R}$ を示す．そのためにまず $\alpha_n = [a_{n,p}]$ $(p \in \mathbb{N}, a_{n,p} \in \mathbb{Q})$ と表す．1. によって $\lim_{p\to\infty} a_{n,p} = \alpha_n$

である．故に

$$\exists p(n); |\alpha_n - a_{n,p(n)}| < \frac{1}{n}$$

そこで $a_n = a_{n,p(n)}$ と置けば $\{a_n\}$ $(a_n \in \mathbb{Q})$ は基本列である．

3. $\alpha = [a_n]$ によって $\alpha \in \mathbb{R}$ を定める．この α に対して $\lim_{n\to\infty} \alpha_n = \alpha$ が証明される． ‖

このようにして順序を導入された $\mathbb{R}$ のことを実数体と呼ぶのである．実数体を公理的に述べれば次のようである：

実数体の特徴付け　完備性を持つ順序体 K は**実数体**と呼ばれる．

[注意]　体 K が**順序体**であるとは，体 K が全順序 $\leqq$ を持ち，

1. $x \leqq y \Longrightarrow x + z \leqq y + z$
2. $x \leqq y,\ z > 0 \Longrightarrow xz \leqq yz$

を満たすことをいう．

定理 4.4　実数体は同型を除いてただ一つ存在する．

同型性の定義は第 7 章に譲るが，その精神を言えば，形式上同一視できるということである．

結果から見れば，無限小数の全体を実数体と呼んでいるにすぎないことがわかる．それなら何故最初から無限小数を実数と呼ぶことにしないのか，という疑問を読者は持たれるに違いない (少くとも私は学生の頃実数論を習ったときそのように思った)．一つには無限小数は 10 進法という特定の表記に頼っているという問題点があろう．他の進法でも同じだという説明が必要である．次に無限小数同士の四則を定義しなければならないが，やってみれば結局は上述と同じ程度の議論が必要になる．読者自らこの辺りを考えてみてもらいたい．

以上一部簡略であったが，こまかい証明にこだわらず気分がわかってもら

えれば良いのだ．同じ数に収束することになる予定の数列を一まとめにして一つのものと考えるという点は抽象数学の精神をよく象徴していて印象的であろう．なお，カントル自身は一つの実数を定めるのにいくつもの数列がある点でデデキントの切断という方法には劣るが，自分の方法は具体的という点で優れていると考えていたそうである．

かくして実数という概念は，個数とか，連続量とか，直線という直観に頼る存在から数千年を経てやっと論理的に厳密に確立されたのである．

§ 2.2　有理数体の構成

有理整数環 $\mathbb{Z}$ から有理数体に到る話も類別で説明できるのだが，極めて有用な考え方だから単に有理数体を説明するだけではなく，一般化しながら実行することにしよう．

定義　環 R が (0 以外の) **零因子**を持たないとき，すなわち

$$ab = 0 \Longrightarrow a = 0 \vee b = 0$$

が R で成り立つとき，R は**整域** (domain) をなすといわれる．

$\mathbb{Z}$ は整域である．$m(\in \mathbb{N})$ が合成数のときは $\mathbb{Z}/m\mathbb{Z}$ は整域ではない．$m = m_1 m_2, m_1 \neq 1, m_2 \neq 1$ とすると $\mathbb{Z}/m\mathbb{Z}$ において $\overline{m_1} \neq \overline{0}, \overline{m_2} \neq \overline{0}$，しかるに $\overline{m_1} \cdot \overline{m_2} = \overline{m_1 m_2} = \overline{0}$ となるからである．p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ は整域である．さらに一般に体は整域である．体では 0 以外は (乗法) 逆元を持つからである．

定理 4.5　環 R を含むような体が存在するための必要十分条件は R が整域であることである．整域 R を含む最小の体を R の**商体**という．

証明　$R \subsetneqq F$ なる体 F が存在すれば，F には零因子が存在しないから R にももちろん存在しない．故に R は整域である．

逆に R が整域であるとしよう．R を含む体を作る．$R^{\times}$ によって $R -$

$\{0\} = \{x(\in \mathbb{R}) \mid x \neq 0\}$ を表す．$\mathfrak{R} = R \times R^{\times}$ とする：

$$\mathfrak{R} = \{(a,b) \mid a \in R, b \in R, b \neq 0\}$$

$\mathfrak{R}$ において $\sim$ を

$$(a,b) \sim (a',b') \Longleftrightarrow ab' = a'b$$

で定義する．$\sim$ が同値律を満足することは容易に知られる．$\mathfrak{R}/\sim$ を $\widetilde{R}$ で表す．$\mathbb{Z}$ と $\mathbb{Q}$ の関係からのアナロジーで (a,b) の属する類を a/b と表す：

$$\overline{(a,b)} = a/b$$

$$\therefore \quad a/b = a'/b' \Longleftrightarrow ab' = a'b$$

$\widetilde{R}$ において

$$a/b + a'/b' = (ab' + a'b)/bb',$$
$$a/b \cdot a'/b' = aa'/bb'$$

によって和と積を定義する．

問題　$\widetilde{R}$ は環をなすことを証明せよ．

写像 $\varphi : R \longrightarrow \widetilde{R}$ を $\varphi(x) = x/1$ によって定義する．ここに 1 は R の乗法単位元とする．$\mathbb{Z}$ の例で言えば $x \in \mathbb{Z}$ に対し分数 $x/1 \in \mathbb{Q}$ を考える．しからば φ は単射，つまり 1 対 1 写像である．なぜなら，$\varphi(a) = \varphi(b)$ は $a/1 = b/1$ を意味する．　$\therefore\ a \cdot 1 = 1 \cdot b$　$\therefore\ a = b$ だからである．

さらに

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b)$$

も容易に確かめられるから R と $\varphi(R)$ とは環として全く同一の構造を持っている．そこで R と $\varphi(R)$ を同一視する．$\mathbb{Z}$ の例で言えば整数 a を分数 $a/1$ と同じものと考える．

ところで $\widetilde{R}$ は体である．なぜなら $\widetilde{R}$ の加法単位元 0 は正確に書けば 0/1 であるが，$a/b \neq 0/1$，すなわち $a \neq 0$ ならば

$$b/a \cdot a/b = 1/1 = 1 \quad (= \text{乗法単位元})$$

だから $\widetilde{R}$ の 0 でない元はすべて逆元を持つのである．故に $R \subseteqq \widetilde{R}$ で $\widetilde{R}$ は体である．$\widetilde{R}$ の最小性は明らかである．‖

§ 3. 素イデアルと極大イデアル

R を環とする．R のイデアル $P(\neq \{0\}, R)$ が**素イデアル**であるとは，$a, b\ (\in R)$ に対して

$$ab \in P \Longrightarrow (a \in P) \vee (b \in P)$$

が成り立つことをいう．

定理 4.6　P が素イデアルであるためには R/P が整域となることが必要十分である．

証明　P が素イデアルであるとする．$\overline{a}, \overline{b} (\in R/P)$ に対して $\overline{a} \cdot \overline{b} = \overline{0}$ が成り立っているとしよう．すると剰余類の積の定義から $\overline{ab} = \overline{0}$ を得る．

$$\therefore\quad ab \in P \qquad \therefore\quad a \in P \vee b \in P \qquad \therefore\quad \overline{a} = \overline{0} \vee \overline{b} = \overline{0}$$

故に R/P は整域である．次を見れば証明が終わる．‖

問題　逆に R/P が整域ならば P は素イデアルであることを示せ．

次に R のイデアル $M(\neq R)$ が**極大イデアル**であるとは，イデアル A に対して

$$M \subseteqq A \subseteqq R \Longrightarrow (A = R) \vee (A = M)$$

が成り立つことをいう．M を含む $(M, R$ 以外の$)$ イデアルは存在しないということである．

定理 4.7　M が極大イデアルであるためには R/M が体となることが必要十分である．

証明　M が極大イデアルであるとする．$\overline{a} \neq \overline{0}$ に逆元が存在することを示せばよい．$a \notin M$ であるからイデアル $M' = \{xa + y \mid x \in R, y \in R\}$ は

$$M \subsetneqq M' \subseteqq R$$

を満たす．M の極大性により $M' = R$．故に $1 \in M$ だから

$$xa + y = 1$$

となる $x \in R, y \in M$ が取れる.

$$\therefore \quad \overline{xa} = \overline{1} \qquad \therefore \quad \overline{x} \cdot \overline{a} = \overline{1}$$

故に $\overline{a}$ は逆元 $\overline{x}$ を持つ. 逆は演習問題とする. ‖

問題　R/M が体であれば M は極大イデアルであることを示せ.

定理 4.8　極大イデアルは素イデアルである.

体は整域でもあるから証明するまでもない. ただ逆は成り立たない.

例　$R = \mathbb{R}[X, Y]$ とする. $P = (X)$ は素イデアルであるが $P \subsetneqq (X, Y) \subsetneqq R$ であるから極大ではない.

証明　(X) が素イデアルであることを示そう. $f, g \in R$ に対して $fg \in (X)$ とすれば $fg = Xh$ となる $h \in R$ が取れる.

$$\therefore \quad f(0, Y)g(0, Y) = 0 \cdot h(0, Y) = 0$$

$$\therefore \quad f(0, Y) = 0 \quad \text{または} \quad g(0, Y) = 0$$

すなわち $f(X, Y)$ か $g(X, Y)$ の一方は X で割れる. 故に P は素イデアルである.

あるいは, 同型という概念を後に説明するが, それを先取りして次のように考えてもよい：

$$R/P \simeq \mathbb{R}[Y]$$

$\mathbb{R}[Y]$ は整域ではあるが体ではない. 故に P は素イデアルだが極大イデアルではないといえる. また

$$R/(X, Y) \simeq \mathbb{R} \quad (\text{体})$$

故に (X, Y) は極大イデアルであることがわかる.

有理整数環 $\mathbb{Z}$ において素イデアル，極大イデアルを考察してみよう．まず $\mathbb{Z}$ は単項イデアル環 (単項イデアル整域) であることに注意しよう．

$(p), p \in \mathbb{N}$ が $\mathbb{Z}$ のイデアルで $(p) \neq \mathbb{Z}$ であるとする．これは $p \neq \pm 1$ というのと同値である．$a, b(\in \mathbb{Z})$ に対して

$$ab \in (p) \Longrightarrow a \in (p) \vee b \in (p)$$

とは

$$p \mid ab \Longrightarrow p|a \vee p|b$$

というのと同じである．((p) とは p の倍数の集合だったから．)

次に $(m), (a), a \in \mathbb{N}, m \in \mathbb{N}$ に対して

$$(m) \subseteqq (a) \subseteqq \mathbb{Z} \Longrightarrow (a) = (m) \vee (a) = \mathbb{Z}$$

は，$\mathbb{Z} = (1)$ だから

$$a|m \Longrightarrow a = m \vee a = 1$$

と同じである．だから自然数の範囲で考えると，

$$(p) \text{ が素 } \equiv (p \neq 1) \wedge (p|ab \Longrightarrow p|a \vee p|b) \tag{8}$$

$$(m) \text{ が極大 } \equiv (m \neq 1) \wedge (a|m \Longrightarrow a = m \vee a = 1) \tag{9}$$

がわかった．何か妙なことに気付かないであろうか．学校の教科書では素数の定義は (9) の右辺だった筈だが？

実は単項イデアル整域では以下に示すように「(8)$\Longrightarrow$(9) が成り立つので，別に騒ぎ立てる程のこともないのだが，p が素数ということの定義を (8) の右辺に変える方が現代代数学と整合的になるだろう：

定義　R を整域とする．$p \in R$ が 0 でなく，また p が生成する単項イデアル (p) が $R = (1)$ と一致しないとする．

1. 任意の a, $b \in R$ に対して $p|ab \Longrightarrow p|a \vee p|b$ が成り立つとき，p は**素元**であると言う．

2. 任意の $a \in R$ に対して $a|p \Longrightarrow (a) = R$, または $(a) = (p)$ が成り立つとき，p は**既約元**であると言う．

こうすれば

$$(p) \text{ が素イデアル} \iff p \text{ が素数}$$

となって気持ちが良い．また，$\mathbb{Z}$ の場合と同様にして，R が単項イデアル整域ならば，

$$(p) \text{ が極大イデアル} \iff p \text{ が既約元}$$

が成り立つ．さらに先に予告したように，次が成立する：

定理 4.9　単項イデアル整域では，素元であることと既約元であることは同値である．

証明　R を単項イデアル整域とし，p を R の既約元とすると，上述のように (p) は極大イデアルである．したがって (p) は素イデアルであるので，p は素元である．

逆に，p を R の素元としよう．$a|p$ が成り立っていると仮定すると，$p = ab$ $(a,\ b \in R)$ と書ける．これは $1 \cdot p = ab$ ともみなせるので，$p|ab$ である．p は素元だから，$p|a$，または $p|b$ である．前者であれば，$a = c \cdot p$ と書けるから，

$$p = ab = (cp)b \quad \therefore \quad bc = 1 \quad \therefore \quad a \in (p) \land p \in (a) \quad \therefore \quad (a) = (p)$$

また後者であれば，同様の手続きで，$(a) = R$ が示せる．これによって，p が既約元であることが証明された．∥

さて，懸案の $\mathbb{Z}$ における素因数分解とその一意性の問題を解決しよう：

定理 4.10 (初等整数論の基本定理)　1より大なるすべての自然数は有限個の正の素数の積に分解される．また順序を除けば，その分解は一意的である．

証明　分解の可能性について．

素因数分解ができないような自然数があるとして，その全集合を X とする．X の中の最小数を m とする．$m \in X$ は素数ではないから，上述の定理

によって既約でもない．既約数の定義の否定形を作ってみると，

$$\exists a\ (\in \mathbb{Z})[a|m \wedge a \neq 1 \wedge a \neq m]$$

であることがわかる．この a に対しては $m = ab$ と書けるが，このとき上式から $a < m$, $b < m$ であることがわかるから，m の選び方 (最小性) によって，a, b はともに素因数分解が可能なはずである．したがって m もそうであることになって，矛盾が生じる．故に $X = \phi$ である．

一意性について．

$$n = p_1 \cdots p_s = q_1 \cdots q_t$$

と二通りに素因数分解されるとしよう．$p_1|n$ と p_1 が素数なることによって $p_1|q_j$ となる j がある．番号を付け換えて $j = 1$ としよう：$p_1|q_1$

$$\therefore \quad \exists a \in \mathbb{N};\ q_1 = ap_1$$

q_1 も素数ゆえ $q_1|p_1 \vee q_1|a$．前者ならば $p_1 = q_1$．後者ならば $\exists b \in \mathbb{N}; a = bq_1$．$\therefore\ q_1 = bp_1q_1 \quad \therefore\ bp_1 = 1$ となり矛盾．以上で $p_1 = q_1$ が示された．

$$\therefore \quad p_2 \cdots p_s = q_2 \cdots q_t$$

これを続ければ $s = t$ であることがわかり，適当に番号を付け換えて $p_1 = q_1, \cdots, p_s = q_s$ を得る．‖

第5章　ユークリッド整域

§1. 論理型と情緒型

数学をやっている人には推理小説の愛好者が多い．本格物といわれる推理小説にしたって少しも論理的ではないのだが，他の小説類，たとえばSFよりは論証好きの人の肌に少しは合っているのだろうか．

私は，というと，大量に読んでいる割には好きでない．何となく肌のザラつくような，いわゆる潤いのない感触が推理小説全体のイメージにまつわりついているからだ．それよりはよく出来た(それが難しい注文なのだが) SFの方が肌に合っている．そう言えばSFは嫌いだと明言する数学者が多いが，これは少し誤解もあるようである．SFという言葉から荒唐無稽なエセ科学主義的メチャクチャ空想小説を連想するのはある意味では当っているのだが，もちろん別の意味ではまったくの間違いである．

空想や虚構が下らないというのなら小説はすべて下らないということになる．実際，小説よりは歴史物やドキュメンタリー，内幕物が好きだという人が多いが，その人達がSFは嫌いだというのなら首尾一貫している．しかし割に純文学や古典を好きな人がSFを好きでないというのは，優れたSFを読んだことのないことに起因する誤解に過ぎない．たとえば鏡を通って死の王女に会いに行くJ. コクトーの『オルフェ』は幻想性という意味において立派にSFで，たとえば，目で見るという限度を越えた，人の理解と表現を越

えた「暗黒それ自身」といった代物をあくことなく描写し続ける背徳の香り高い C.L. ムーアの Northwest Smith 物 (ムーアは女性の SF 作家) と同じ系譜に数えても良いのである．また，小人になったら，巨人になったら，そしてもし馬からみれば人間がいかに醜怪な生き物に見えるかをしつこく描写するスウィフトの『ガリバー旅行記』は，視点を変えて事柄を見るという SF の代表的手法の実例であって，ある星の昆虫的生物には人類の母親が自分の赤ん坊に向ける愛情の奔流がギャーッと気も狂うほどの生温かい気持ち悪さに感じられたという話の “The Deep”(SF の代表的作家アシモフの短編) と軌を一にしていることが理解されよう．実際純然たる宇宙ものでもない限り SF とはこういうものという限定は出来ないのである．

なお，『ガリバー旅行記』とか『ドン・キホーテ』と言えば子供の頃に話を聞いているのが災いして本物を読まないものの双璧だが，実際は子供の読物ではないばかりかどちらも最高の文学作品である．『ドン・キホーテ』などはドストエフスキーが有史以来最高の傑作だとまで称賛したものだ．(『白痴』は『ドン・キホーテ』をまねて書かれたものだそうな.) フェルマーの大定理なんどに凝って身心を破滅させていないでこんなオモロイ小説でも読んだらどうや，と言いたい．

SF の弁護はこれ位にして話を進めよう．数学者の大半は

推理小説好き，歴史物・実証物好き，碁・将棋・オセロゲームなどが強い

というパターンに属するように思う．一方，

SF 好き，文学好き，夢想好き，論理性を持つ勝負事が弱い

というパターンもあり，数学の世界では少数派に属する．前者を論理型と呼ぼう．後者は情緒型と名付ける．

詩人味を持ち合せない大数学者はいない (ワイエルシュトラス) ともいうし，どれにでもちょっとずつ口を出したがる私のごとき人間もいるから，二つの型が完全に排反的でないことは確かである．しかしまた碁の強い大詩人な

んて詩を書かない詩人のような矛盾的響きを持っていることからしてもある程度は排反的ではあるだろう．(萩原朔太郎と宮沢賢治のいずれか一方でも碁が強かったということが判明すれば「碁の強い大詩人なんてありえない」という言葉は撤回する．というのは私が大詩人と呼ぶのはこの二人だけだから．)

私は先ほども言ったように何にでも口を出したがるたちだが，本質的には情緒人間である．一見そうでなく見えるのは努力の賜である．碁に関しても，好きは好きだが努力の割には弱い，そして碁の強いタイプの人間にはイヤな奴が多いと思っている．(プロの碁打に向って「あなたは碁が強いですね」とはいわない．碁が強いというのはしたがって素人のことである．)

情緒型人間は数学に向いているとは言い難い．したがって私などはもっとも素質のない口でいつになったら数学をやめる口実ができるかばかり考えているといってもよい．じゃ何に向いているかというと，とくにこれといって特別なものはないのであって，あれに凝ったりこれに凝ったり振動を続けながら楽しく過していきたいというにすぎない．

私のように数学の素質のない人間でも，一通り理解出来るところにまでは「努力」の二字によって達することが可能であるとは思う．数学がわかるようになる要点は，第一にはセミナーなどで，徹底的に隅から隅まで，一冊のテキストを丸暗記するほどていねいに読むこと，第二には，それ以外の分野は可能な限り人に聞いて何となく全貌を理解するようにする，という二つの相反する要素があるように思う．一つの自分の収めたい題目は隅から隅まで，しかしそれ以外の分野は小説を読むように全体像を理解するのである．それから，大切なのは，自分で考えるだけではだめだということである．また，脇目を振らず本を読んでいるだけでもいけない．この要領は案外むずかしい．

大学で先生や先輩と一緒にいるメリットは，雰囲気を身につけることができることに尽きるだろう．独学だとどうしても，どうでも良いような細部にこだわり袋小路に入り込むことが多く，逆に重要なカンドコロを見過ごしてしまったりするものである．こんな言葉が『論語』にある：

学びて思わざるは則ち罔(くら)く，思いて学ばざれば則ち殆(あやう)し (為政篇)

「殆」はまた「疑う」とも訓(よ)むそうな．ある人が「罔」と「殆」とを入れ換えた方が正しいと書いていたが，「殆」を「あやうし」とよむ場合はそうかもしれない．

一つの分野が解るようになると他の分野はちょっとした努力で解るようになる傾向があるから，最初から傾向の違うものを学んではいけない．というのにも『論語』に

異端を攻(おさ)むるべからず

という言葉がある．貝塚茂樹さんが，巻物を両方から巻いていってはならない，そういう学び方をしてはならないという風に解釈していたが，それが今の例に当たる．

§ 2.　ユークリッド整域

定理 4.10 の証明を子細に調べれば割算の原理が形式的に成り立てば単項イデアル整域になるだろうということや，一意的な素元分解が成り立つことが予想される．これはわれわれにとってきわめて都合のよいことなので，こうした整域について調べてみることにしよう．

定義　R を整域，すなわち零因子を持たない可換環とし，$R^{\times} = \{x(\in R) \mid x \neq 0\}$ とする．次の条件を満足する写像 $N : \mathbb{R}^{\times} \longrightarrow \mathbb{N} \cup \{0\}$ が存在するとき R は**ユークリッド整域** (略して E.D.) と呼ばれる：

1. $N(ab) \geqq N(a) \quad (\forall a \forall b \in R^{\times})$
2. $a, b \in R \quad (a \neq 0)$ に対して

$$b = qa + r, \quad (r = 0) \vee (N(r) < N(a))$$

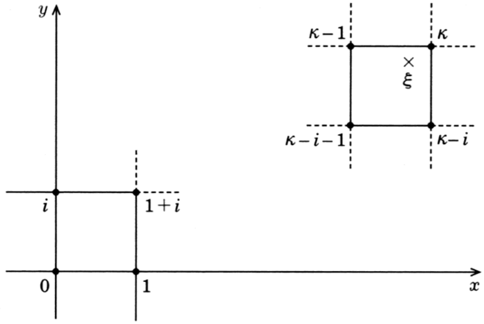
なる $q, r(\in R)$ が存在する．

例　$\mathbb{Z}$ は $N(x) = |x|$ と定義すれば E.D.(ユークリッド整域) である．また F が体のとき，F 上の 1 変数多項式環 $F[X]$ は $f \in F[X]$ に対して $N(f) = \deg f$(f の次数) と定義すれば E.D. となる．

この二つの例から E.D. というのは割算の原理の成り立つ環の抽象化であることがわかる．

定理 5.1　$\mathbb{Z}[i]=\{x+yi \mid x,y\in\mathbb{Z}\}$，ここに $i^2=-1$，は $N(\alpha)=|\alpha|^2$ $(\alpha\in\mathbb{Z}[i]^{\times})$ と定義すれば E.D. である．

証明　$\alpha,\beta\in\mathbb{Z}[i],\alpha\neq 0$ とする．$\xi=\beta/\alpha$ と置くと $\xi\in\mathbb{Q}[i]=\{x+yi \mid x,y\in\mathbb{Q}\}$ である．$\mathbb{Z}[i]$ に属する数は複素平面上で図示すると一辺の長さが 1 の正方格子をなしている．



ξ が含まれる正方形を取って考えれば，その 4 頂点のうち少なくとも一つから ξ までの距離は 1 より小さい．その頂点を κ とすれば $\kappa\in\mathbb{Z}[i]$ であって，$|\xi-\kappa|<1$ が成り立つ．

$$\therefore\ \left|\frac{\beta}{\alpha}-\kappa\right|<1 \quad \therefore\ |\beta-\kappa\alpha|<|\alpha|$$

そこで $\beta-\kappa\alpha=\rho$ と置けば $\rho\in\mathbb{Z}[i]$ で

$$\beta=\kappa\alpha+\rho,\ (\rho=0)\vee(|\rho|<|\alpha|).$$

条件 1 は $N(\alpha\beta)=N(\alpha)N(\beta)$ かつ $N(\alpha)\in\mathbb{N}$ だから成り立つ．∥

定理 5.2　$\rho=\dfrac{-1+\sqrt{3}i}{2}$ とすれば $\mathbb{Z}[\rho]$ は E.D. である．

問題　定理 5.2 を定理 5.1 に準じて証明せよ.

[注意]　$\mathbb{Z}[\sqrt{3}i]$ は E.D. ではない.

$\mathbb{Z}[\alpha]$ (ただし α は $\alpha^2 + a\alpha + b = 0$ という形の整数係数の既約 2 次方程式の根) という形に表せる整域でユークリッド的となるものは上例の他には $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}]$ など有限個しか存在しないことがわかっているので，素元分解の問題は E.D. であるかどうかだけに頼るわけにはいかない難問である.

定理 5.3　E.D. (ユークリッド整域) は P.I.D. (単項イデアル整域) である.

問題　定理 5.3 を証明せよ.

[ヒント]　$\mathbb{Z}$ や $F[X]$ のときと同じである. イデアル $A \neq (0)$ の元の中で $N(\alpha)$ が最小の元 α を選ぶと $A = (\alpha)$ となるのである.

定義　環 R において元 $\alpha(\neq 0)$ が元 β を**割り切る**とは

$$\exists\gamma(\in R); \beta = \gamma\alpha$$

が成り立つときにいう. 記号 $\alpha|\beta$. このときまた α は β の**約元** (**約数**) であるともいう.

問題　$\alpha|\beta \Longleftrightarrow (\beta) \subseteqq (\alpha)$ を証明せよ.

定義　環 R において 1 の約元を**単元**あるいは**ユニット**という. $R \subseteqq \mathbb{C}$ のときは**単数**というのが普通である：

$$\varepsilon(\in R); \text{単元} \Longleftrightarrow \exists\eta(\in R); \varepsilon\eta = 1$$

次に $\pi(\in R)$ が 0 でも単元でもないとする.

$$\pi|\alpha\beta \Longrightarrow \pi|\alpha \vee \pi|\beta$$

が満たされるとき π は R の**素元**であると呼ばれる. これはイデアル (π) が素イデアルであることと同値である.

問題　$\mathbb{Z}$ の単数は ± 1 だけである．F を体とするとき環 $F[X]$ の単元は $F^{\times}$ である．$\mathbb{Z}[i]$ の単数は $\pm 1, \pm i$ の四つである．$\mathbb{Z}[\rho]$ の単数は ± 1, $\pm \rho$, $\pm \rho^2$ の六つである．

問題　環 R の単元の全体 U は乗法群をなす．

体においては 0 以外の元はすべて単元である．これは当り前だが初めのうちは戸惑い勝ちなので老婆心で一言述べておく．

問題　環 R において $(\alpha) = (\beta) \Longleftrightarrow \exists \varepsilon \in U; \varepsilon\alpha = \beta$ を証明せよ．このとき α と β は**同伴**であるという．

補題　R が E.D. のとき，次が成り立つ：

1. N の像 $N(R^{\times})$ の中で，$N(1)$ は最小である．
2. $N(\alpha) = N(1) \Longleftrightarrow \alpha \in U$
3. $(\alpha) = (\beta) \Longleftrightarrow N(\alpha) = N(\beta) \wedge \alpha | \beta$

証明　1. $\alpha = 1 \cdot \alpha$ より $N(\alpha) \geqq N(1)$ を得る．

2. $N(\alpha) = N(1)$ とせよ．$1 = q\alpha + r$, $(r = 0) \vee (N(r) < N(\alpha))$ と表せるが，$N(\alpha)$ の最小性によって $r = 0$ でなければならない．ゆえに $\alpha \in U$ である．

3. $\beta = \varepsilon\alpha$, $\varepsilon \in U$ ならば，E.D. の第 1 条件によって，$N(\beta) \geqq N(\alpha) \geqq N(\beta)$ であるから，$N(\alpha) = N(\beta)$ を得る．逆に $N(\alpha) = N(\beta) \wedge \alpha | \beta$ とせよ．

$$\alpha = q\beta + r, \quad (r = 0) \vee (N(r) < N(\beta))$$

と表す．仮定から $\beta = \gamma\alpha, \gamma \in R$ と表せるから

$$r = \alpha - q\beta = \alpha - q\gamma\alpha = \alpha(1 - q\gamma).$$

故に，E.D. の条件 1. によって $r \neq 0$ なら $N(r) \geqq N(\alpha) = N(\beta)$ となるので，矛盾を生じる．故に，$r = 0$ である．これによって $(\alpha) = (\beta)$ を得る．‖

この補題があれば，次の定理の証明は $\mathbb{N}$ の場合とまったく同じに運ぶことができる：

定理 5.4　ユークリッド整域においては，0 でないすべての元が有限個の素元の積に分解される．しかもその分解は一意的である．すなわち

$$\alpha = \pi_1 \cdots \pi_s = \rho_1 \cdots \rho_t$$

を元 α の二通りの素元分解 (つまり，$\pi_1, \cdots, \pi_s, \rho_1, \cdots, \rho_t$ は素元) とすれば $s = t$ で，しかも順序の取り換えによって

$$(\pi_1) = (\rho_1), \cdots, (\pi_s) = (\rho_s)$$

とできる．

証明　R が E.D. であるとする．$R^\times$ に素元分解ができないような元があるとして，その全集合を X とする．X の中で N の値が最小の元を α とする．$\alpha \in X$ は素元ではないから，既約でもない (R は単項イデアル整域であることによる)．したがって，

$$\exists \beta\ (\in R)[\beta | \alpha \wedge (\beta) \neq R \wedge (\beta) \neq (\alpha)]$$

このときこの β を使って，

$$\alpha = \beta\gamma, \quad (\gamma) \neq R \wedge (\gamma) \neq (\alpha)$$

と表せるから，補題の 3. によって $N(\beta) < N(\alpha)$, $N(\gamma) < N(\alpha)$ が従う．$N(\alpha)$ の最小性によって β, γ は素元分解可能だから，α も素元分解可能であり，矛盾を生じる．故に $X = \phi$ である．一意性の証明は簡単だから読者に任せよう．∥

素元分解が一意にできる整域を U.F.D. と略する．unique factorization domain の略である．定理 5.4 によって次がわかった：

$$\text{E.D.} \implies \text{U.F.D.}$$

§ 3. $p = x^2 + y^2$ 型の素数

$\mathbb{Z}[i]$ や $\mathbb{Z}[\rho]$ ($\rho^3 = 1, \rho \neq 1$) は U.F.D. であることが証明されたので，これらの結果を初等整数論的な話題に応用してみよう．

まず最初はピュタゴラス数への応用である．

整数 x, y, z に対し

$$x^2 + y^2 = z^2, \quad (x, y) = 1$$

が満たされているとする．

$$(x + yi)(x - yi) = z^2 \tag{1}$$

$x + yi = \alpha, x - yi = \beta$ と置けば $\alpha, \beta \in \mathbb{Z}[i]$ である．

π を $\mathbb{Z}[i]$ の素元とし，$\pi|\alpha, \pi|\beta$ とすれば $\pi|2x, \pi|2yi$．i は単数だから $\pi|2y$．仮に $\pi|2$ とする．一方 $\pi|\alpha$ なのだから $\pi|z^2$．$\therefore$ $\pi|z$．一方 $(2, z) = 1$ だから

$$\exists x', y' (\in \mathbb{Z}); 2x' + zy' = 1$$

$\pi|2, \pi|z$ より π が 1 の約数，すなわち単数となって矛盾する．$\therefore$ $\pi \nmid 2$．故に $\pi|x, \pi|y$ を得る．$(x, y) = 1$ より

$$\exists u, v \in \mathbb{Z}; ux + vy = 1.$$

故に π は 1 の約数となり素元ということに反する．したがって，α と β とは $\mathbb{Z}[i]$ の元として互いに素である (つまり公約素元を持たない)．(1) より

$$\alpha\beta = z^2, \quad \alpha, \beta \text{ は互いに素.}$$

この表現と素元分解の一意性から $\alpha = \varepsilon\gamma^2$，$\gamma \in \mathbb{Z}[i]$，$\varepsilon$ は単数となる．γ を $a + bi$ とすれば

$$x + yi = \varepsilon(a + bi)^2 = \varepsilon(a^2 - b^2 + 2abi)$$

$\varepsilon = \pm 1$ ならば

$$x = \pm(a^2 - b^2), \quad y = \pm 2ab$$

$\varepsilon = \pm i$ ならば

$$x = \mp 2ab, \quad y = \pm(a^2 - b^2)$$

を得る．z はいずれの場合も $\pm(a^2 + b^2)$ である．ただし a, b は偶奇性を異にする．(そうでないと $(x, y) \neq 1$ となってしまう．)

定理 5.5　p を素数とする．

$$p = x^2 + y^2 \quad (x, y \in \mathbb{N}) \tag{2}$$

という形に表せるためには $p = 2$, または $p \equiv 1 \pmod 4$ が必要十分である．

定理の主張は明解だが，証明はやや高度なので，これ以降 §3 の終わりまでは最初は大体を知るだけで良いかもしれない．

証明の前に簡単な考察をしておこう．$p = 2$ なら $2 = 1^2 + 1^2$ である．p が奇素数で (2) のように表せるとすると x, y の一方は偶で，もう一方は奇である．したがって $p \equiv 1 \pmod 4$ は明らかである．問題は逆である．(2) のように表せるということは

$$p = \pi_1\pi_2, \quad \pi_1 = x + yi, \quad \pi_2 = x - yi$$

となるわけで，素数 p が $\mathbb{Z}[i]$ では素元でないことを意味する．イデアルという言葉を使えば $(p) = p\mathbb{Z}[i]$ が素イデアルではない (つまり $\pi_1 \notin (p), \pi_2 \notin (p)$, but $\pi_1\pi_2 \in (p)$) と言い表せる．

証明 (定理の証明)　上の考察によって，p が $\mathbb{Z}[i]$ の素元であるかどうかは $(p) = p\mathbb{Z}[i] = \{pz \mid z \in \mathbb{Z}[i]\}$ が $\mathbb{Z}[i]$ の素イデアルであるかどうかにかかっている．言い換えれば $\mathbb{Z}[i]/(p)$ が整域かどうかである．

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$$

という同型は $X^2 + 1$ が現れるたびに 0 とすることを意味している．それをさらに (p) で類別するということは $a \equiv b \pmod p$ なる係数は等しいと見るということである (正確には，定理 11.9 の証明参照)．すなわち

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1)$$

(ここに $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, (X^2 + 1) = (X^2 + 1)\mathbb{F}_p[X]$ である．)

したがって (p) が素イデアルかどうかは $(X^2 + 1)$ が $\mathbb{F}_p[X]$ で素イデアルかどうかにかかっていることになる．$\mathbb{F}_p[X]$ も U.F.D. であるから，素元でないとは

$$X^2 + 1 = (X + a)(X + b)$$

と分解できることである．係数比較によって $b = -a$ であるから，

$$a^2 = -1$$

が $\mathbb{F}_p$ で解を持つかどうかで決まることがわかる．つまり

$$a^2 \equiv -1 \pmod p$$

が整数解 a を持つことである．これはすなわち平方剰余の相互法則の第一補充法則 (定理 8.7) によって $p \equiv 1 \pmod 4$ が成り立つということである．結局この場合，素数 p は $\mathbb{Z}[i]$ で素元のままということはなく二つの数 ($\neq$ 単数) の積に分解されるのである．∥

以上から次も示せたことになる：

系　素数 p は $\mathbb{Z}[i]$ において次のように素元分解される：

1. $p = 2$ ならば $2 = \varepsilon\lambda^2$，ここに $\varepsilon = i$(単数), $\lambda = 1 - i$.
2. $p \equiv -1 \pmod 4$ ならば p は $\mathbb{Z}$ でも素元である．
3. $p \equiv 1 \pmod 4$ ならば $p = \pi \cdot \overline{\pi}$ と分解する．ここに π は $p = a^2 + b^2$ なる a, b を使って $\pi = a + bi$ と表せる．

$z = x + yi \in \mathbb{Q}(i)$ に対して

$$Nz = (x + yi)(x - yi) = x^2 + y^2$$

と定義し，z の**ノルム**と称する．(解析学では $|z|^2$ と書かれる．) このとき

$$N(z_1 z_2) = Nz_1 \cdot Nz_2$$

は明らかであるが，これを書き下すと

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_2y_1 - x_1y_2)^2 \tag{3}$$

という恒等式になる．(3) はブラフマグプタの恒等式と呼ばれて 7 世紀のころから知られていたことが立証されている．

(3) は実に意味の深い式である．

$$n = p_1^{m_1} \cdots p_r^{m_r}$$

を自然数 n の素因数分解とするとき n が 2 平方和で表せるかどうかは素数の冪 $p_i^{m_i}$ が 2 平方和で表せるかどうかに還元できる，というのが「意味深い」ことの一つである．

さらに (3) は二つの同じ形 x^2+y^2 の 2 次形式の積がふたたび同じ形の 2 次形式とみなせるということも意味している．これは 2 次形式の合成という深い理論に至る道である (第 11 章 §4 参照).

$\mathbb{Z}[\rho]$ が U.F.D. であることを使うと次の定理が示せる．

定理 5.6　p を 3 より大きい素数とする．

$$p = x^2 + 3y^2 \quad (x, y \in \mathbb{N})$$

と表せる条件は

$$p \equiv 1 \pmod 6$$

である．

証明　前定理と考え方は同じなので少し簡略にしよう．

(p) の $\mathbb{Z}[\rho]$ $\left(\rho = \dfrac{-1+\sqrt{3}i}{2}\right)$ における素元分解は $x^2+3 \pmod p$ の分解にかかっている．$p \equiv 1 \pmod 4$ のときは相互法則 (定理 8.6) によって

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$$

だから $p \equiv 1 \pmod 3$ のとき $\left(\dfrac{-3}{p}\right) = 1$．したがって $p \equiv 1 \pmod{12}$ のとき $\left(\dfrac{-3}{p}\right) = 1$ である．$p \equiv -1 \pmod 4$ の場合も同様に計算して $p \equiv 7 \pmod{12}$ のとき $\left(\dfrac{-3}{p}\right) = 1$ となる．両方あわせて

$$\left(\frac{-3}{p}\right) = +1 \Longleftrightarrow p \equiv 1 \pmod 6$$

を得る．このとき

$$X^2 + 3 \equiv (X + a) \cdot (X - a) \pmod{p}$$

と因数分解され，それ以外のとき，つまり $p \equiv -1 \pmod{6}$ のときには $X^2 + 3$ は mod p でも既約である．つまり $\mathbb{Z}[\rho]$ において p は素元のままである．

$p \equiv 1 \pmod{6}$ とする．p は整数だから $\mathbb{Z}[\rho]$ の数 π ($\neq$ 単数) で割り切れれば，π の複素共役数 $\overline{\pi}$ でも割り切れなければならない．p が素数ということから結局 $\pi, \overline{\pi}$ は素元であって

$$p = \pi \cdot \overline{\pi}$$

と因数分解されることになる．

さて $\mathbb{Z}[\rho]$ における数は $x + \rho y$ $(x, y \in \mathbb{Z})$ と表せるのだが，それが $\mathbb{Z}[\rho]$ における単数 $\pm\rho, \pm\rho^2$ を掛けることによって $x' + \sqrt{-3}y'$ $(x', y' \in \mathbb{Z})$ の形に直せることを示そう．α と β とは

$$\exists\varepsilon\,(\text{単数}); \beta = \varepsilon\alpha$$

のとき同伴であると呼ぶのだが，$x + \rho y$ と同伴な $x' + \sqrt{-3}y'$ という形の数があることを示すのである．

y が偶数なら $y = 2y'$ として

$$x + \frac{-1 + \sqrt{-3}}{2} \cdot y = (x - y') + \sqrt{-3}y'$$

で問題ない．

x が偶数なら，$x = 2x'$ として

$$\begin{aligned} \rho^2(x + \rho y) &= y + \rho^2 x \\ &= y + \frac{-1 - \sqrt{-3}}{2} 2x' \\ &= (y - x') - \sqrt{-3}x' \end{aligned}$$

とできる．

最後に，x も y も奇数のときは

$$\begin{aligned} \rho(x + \rho y) &= \rho^2 y + \rho x \\ &= -\frac{x + y}{2} + \frac{x - y}{2}\sqrt{-3} \end{aligned}$$

となり，これも OK である．

以上によって π あるいは $\rho\pi$ あるいは $\rho^2\pi$ は $\mathbb{Z}[\sqrt{-3}]$ の元となることがわかった．しかも

$$\rho\pi \cdot \overline{\rho\pi} = \pi\overline{\pi} = p$$

また

$$\rho^2\pi \cdot \overline{\rho^2\pi} = \pi\overline{\pi} = p$$

だから，p は $p \equiv 1 \pmod 6$ のとき

$$\begin{aligned} p &= (x+\sqrt{-3}y)(x-\sqrt{-3}y) \\ &= x^2 + 3y^2 \end{aligned}$$

と表せることになる． ‖

§ 4. P.I.D. は U.F.D. か？

この節では

$$\text{P.I.D.} \implies \text{U.F.D.}$$

の証明を試みる．その証明にはちょっとした心配りの足りない個所があるのだが，それがどういうことなのかを説明したい．

定理 5.7　単項イデアル整域では素元分解が一意的に行なえる．

証明　R を P.I.D. とする．素元の有限個の積として表せない $R^\times$ の元の全体を M としよう．(単元は 0 個の素元の積と考えるから M の元ではない.)　$\alpha \in M$ とすると $\exists \alpha_1, \alpha_1' (\in R)$；

$$\alpha = \alpha_1\alpha_1',\ (\alpha) \subsetneqq (\alpha_1),\ (\alpha) \subsetneqq (\alpha_1')$$

が成り立つ．なぜなら，(α) が極大イデアルなら α は素元だし，(α) が極大イデアルではないとすると $(\alpha) \subsetneqq (\beta) \subsetneqq R$ なる β が存在し，$\alpha = \beta\gamma$ と表せるからである．

ところが α_1, α_1' の少なくとも一方は M の元である．何故なら，両方とも M に属さぬということは共に素元の有限積と表せることを意味し，したがって α もそうなるからである．そこで $\alpha_1 \in M$ としよう．α_1 も同様に

$$\alpha_1 = \alpha_2\alpha_2', \ (\alpha_1) \subsetneqq (\alpha_2), \ (\alpha_1) \subsetneqq (\alpha_2')$$

という分解が可能である．この作業を続けて (厳密には数学的帰納法によって) $R^\times$ の元の列 $\{\alpha_n\}_{n=1}^\infty$ で性質

$$(\alpha) \subsetneqq (\alpha_1) \subsetneqq (\alpha_2) \subsetneqq \cdots \subsetneqq (\alpha_n) \subsetneqq (\alpha_{n+1}) \subsetneqq \cdots \tag{4}$$

を持つものが取れる．

$$A = \bigcup_{n=1}^{\infty} (\alpha_n) = \{x(\in R) \mid \exists n \in \mathbb{N}; x \in (\alpha_n)\}$$

と置くと A は R のイデアルをなす．(**問題**　A がイデアルをなすことを証明せよ.)

R は P.I.D. だから $A = (\beta)$ なる $\beta \in R$ が存在する．しかるに $\beta \in A$ だから A の定義から $\beta \in (\alpha_m)$ を満たす m があるはずなので $(\beta) \subseteqq (\alpha_m)$ を得る．$\therefore$ $A = (\alpha_m)$．故に

$$(\alpha_m) = (\alpha_{m+1}) = \cdots$$

となって (4) に反する．この矛盾は $M = \varnothing$ を意味する．

以上で素元分解の可能性が示せた．一意性の方は E.D. の場合，したがって $\mathbb{Z}$ の場合と同じだから省略．‖

流通する代数学の教科書のほとんどすべてでこれが証明としてまかり通っているが，上の証明は厳しいことを言うと不注意な点がある．その不備を見抜いて頂きたい．先に答を述べておくと，ここでは本当は選択公理が必要とされるのである．

The kind of argument just given is used by most mathematicians, since it seems to be easier to find than a more proper argument. The reader should probably employ such arguments himself and at the same time know how to replace them by arguments using the Axiom of Choice. (Vaught[15])

第6章　選択公理について

§1. 選択公理

前章で「P.I.D. $\Longrightarrow$ U.F.D.」の証明には不備がある，あるいは少くともそれが自覚されていないという指摘をした．実は「厳密には数学的帰納法によって」が「厳密には」数学的帰納法によるのではなく，選択公理によるのである．このことを説明しよう．そのために，数学的帰納法とは一体何であるか．まずこの原点に立ち戻って考えてみよう．

数学的帰納法の原理　自然数 n についての命題 $P(n)$ に対して，

1. $P(1)$ は正しい，

2. 任意の自然数 k に対して，$P(k)$ が正しいならば $P(k+1)$ も正しい．

の二つが証明されるならば，すべての自然数 n について $P(n)$ は正しい．

さて，もしも定理 5.7 の推論が正しいならば次の推論も正しいはずである：

$A_1, \cdots, A_n, \cdots$ を空でない集合の系とする．

$$\prod_{n=1}^{\infty} A_n$$

によって $A_1, \cdots, A_n, \cdots$ の**直積**を表す．すなわち $\mathbb{N}$ から $\bigcup_{n=1}^{\infty} A_n$ への写像 f のうち $f(n) \in A_n (n = 1, 2, \cdots)$ を満足するものの全体を $\prod_{n=1}^{\infty} A_n$ とする；

$$\prod_{n=1}^{\infty} A_n = \left\{ f : \mathbb{N} \longrightarrow \bigcup_{n=1}^{\infty} A_n \mid f(n) \in A_n \ (\forall n \in \mathbb{N}) \right\}$$

あるいは列 $\{a_n\}_{n=1}^{\infty}$ で $a_n \in A_n$ を満足するものの全体と言えばわかり良いだろうか．このとき

$$\prod_{n=1}^{\infty} A_n \neq \varnothing$$

が成り立つ．

証明　$A_1 \neq \varnothing$ なので $a_1 \in A_1$ なる a_1 が取れる．列 $a_1, a_2, \cdots, a_n$ が選ばれたとする．$A_{n+1} \neq \varnothing$ だから $a_{n+1} \in A_{n+1}$ なる a_{n+1} が取れる．したがって数学的帰納法によってすべての自然数 n に対して a_n が選べる．故に列 $\{a_n\}_{n=1}^{\infty}$ が存在し $\prod_{n=1}^{\infty} A_n \neq \varnothing$ が証明された． ||

この証明の中で n に関する命題 $P(n)$ とは一体何か？　を考えて頂きたい．さて何だろう？　$P(n) \equiv \left(\prod_{k=1}^{n} A_k \neq \varnothing \right)$ であろうか，$P(n) \equiv (A_n \neq \varnothing)$ ででもあろうか．いずれにしても

$$\prod_{k=1}^{n} A_k \neq \varnothing \ (\forall n \in \mathbb{N}) \Longrightarrow \prod_{k=1}^{\infty} A_k \neq \varnothing$$

が全くのナンセンスであることは今や読者にとっても明らかであろう．

さて選択公理とは何かというと，この $\prod_{n=1}^{\infty} A_n \neq \varnothing$ が選択公理そのものなのである：

選択公理 (Axiom of Choice：AC と略する)　$\{A_j\}_{j \in I}$ $(I \neq \varnothing)$ を集合系 (集合の集合) とする．

$$\prod_{j \in I} A_j = \left\{ f : I \longrightarrow \bigcup_{j \in I} A_j \mid f(j) \in A_j \ (\forall j \in I) \right\}$$

と定義するとき，

$$A_j \neq \varnothing \ (\forall j \in I) \Longrightarrow \prod_{j \in I} A_j \neq \varnothing$$

である．すなわち，I 上で定義された $f(j) \in A_j$ $(\forall j \in I)$ を満たす写像 (選

択関数) f が存在する.

こんな声が聞えてくるような気がする.「そこまで言うなら，集合の集合って何だ ?」確かに「集合の集合」というのは同じ言葉が重なってイヤな感じであるが，逆に，先に集合が与えられたとしよう．その元が集合であるというのはごく普通の現象である．類別をくり返して数体系を作っていったことなどを思い出せば，実例にはこと欠かない．要するに，集合を元として集合を作るのか，集合の元が集合であるのか，見方の違いである．こうしたことから公理的集合論では，すべての対象は集合であるということにして煩雑さを避けることになったのだろう.

選択公理を AC と略記する．AC は添字集合 I が $\mathbb{N}$ の場合でも数学的帰納法によって証明されないことは上述の通りである．なお $I = \mathbb{N}$ の場合，AC は**可算選択公理**と呼ばれている．どんなに懐疑的な人でも可算選択公理は認めないと数学にならない.

AC のもう一つのご利益を説明しよう.

集合 S が空でない部分集合の系 $\{S_\lambda\}_{\lambda\in\Lambda}$ の和集合としてちょうど表されているとする：

$$S = \bigcup_{\lambda\in\Lambda} S_\lambda, \quad S_\lambda \cap S_\mu = \varnothing, \text{ if } \quad \lambda \neq \mu$$

このとき各 $S_\lambda(\lambda \in \Lambda)$ から一つずつ $a_\lambda(\in S_\lambda)$ を選んで代表系 $\{a_\lambda\}_{\lambda\in\Lambda}$ を作ろう．集合というものを単なる「ものの集まり」と考える素朴な立場から言えば $\{a_\lambda\}_{\lambda\in\Lambda}$ が「集合」であることは当り前ということになる．しかし何でもかんでも集合ということにすると色々と不都合が生ずるという理由で少しでも公理的な立場から集合論を考えようとするならば，ものの集まりが「集合」という名前で呼ばれるには何らかの制約を受けねばならない．とこう考えると上の $\{a_\lambda\}_{\lambda\in\Lambda}$ が「集合」をなすということは自明ではない.

$f \in \prod_{\lambda\in\Lambda} S_\lambda$ とする．(AC によって f の存在が保証されている.) f は集合 Λ から集合 $\bigcup_{\lambda\in\Lambda} S_\lambda$ への「写像」なのだから像 $f(\Lambda)$ は $\bigcup_{\lambda\in\Lambda} S_\lambda$ の部分集

合をなすことが分離公理 (p.248 参照) によって保証される．$f(\Lambda) = \{f(\lambda) \mid \lambda \in \Lambda\}$ は $f(\lambda) \in S_\lambda$ だからちょうど代表系そのものである．

このように集合の直和分割から「代表系を選び出せる」というのが AC のご利益である．しかし素朴な立場からみればこれは当然のことなのであって，したがって AC は何ら変わった公理ではないとも言えよう．だから AC を集合論の他の公理と切り離して考えたのではその正確な意味を把握することは難しい．

AC から証明される命題の中でとりわけわれわれに関係が深いのは次である：

依存選択の原理 (Principle of Dependent Choices)　X を集合 $(\neq \varnothing)$ とし，$x \prec y$ を X における関係とする (たとえば $x \leqq y$ とか，$x \mid y$ とか，何でもよい)．もしも任意の $x \in X$ に対して $x \prec y$ を満たす $y \in X$ が常に少なくとも一つ存在するならば，

$$x_1 \prec x_2 \prec x_3 \prec \cdots \prec x_n \prec x_{n+1} \prec \cdots \tag{1}$$

を満たす X の元の列 $\{x_n\}_{n=1}^{\infty}$ が取れる．

この原理が使えるなら，定理 5.7 の証明で，$\alpha \in M$ に対して $(\alpha) \subsetneqq (\beta)$ なる $\beta \in M$ が取れることを示した瞬間に「依存選択の原理によって」

$$(\alpha) \subsetneqq (\alpha_1) \subsetneqq (\alpha_2) \subsetneqq \cdots \subsetneqq (\alpha_n) \subsetneqq (\alpha_{n+1}) \subsetneqq \cdots$$

なる列が存在するということができるのである．つまりは「数学的帰納法によって」と書かずに「依存選択の原理によって」(あるいは「選択公理によって」) と書けばよかったのである．

それでは AC から DC (依存選択の原理) を導いてみよう．

証明　$x \in X$ に対して $A_x = \{y \in X \mid y \succ x\}$ と置く．仮定によって $A_x \neq \varnothing$ $(\forall x \in X)$．故に AC によって集合 $\{A_x | x \in X\}$ の選択関数 $\Phi : X \to \bigcup\{A_x \mid x \in X\}\,(\subseteqq X)$ が存在し，A_x の定義によって $x \prec \Phi(x)$ である．

$$x_{n+1} = \Phi(x_n)$$

と定義すると (1) が成り立つ ($x_1 \in X$ は任意)．　‖

なお，可算無限個の集合を対象とする AC を可算選択公理と呼ぶが，AC, DC との間の強さの関係は

$$\mathrm{AC} \Longrightarrow \mathrm{DC} \Longrightarrow \text{可算 AC}$$

だが，逆方向 $\Longleftarrow$ はいずれも成り立たないことが知られている．だから可算 AC だけしか認めないという立場も取りにくいのである．

なお，数列 $\{x_n\}$ とは $\mathbb{N}$ で定義された写像のことだという立場から見れば，x_n から x_{n+1} を構成する規則が与えられただけでは未だ十全とは言えない．数学的帰納法から関数を定義するには次の回帰定理を必要とすることを一言しておこう：

定理 6.1 (回帰定理)　集合 S の元 a と写像 $f : S \to S$ が与えられたとき，

$$g(1) = a, \quad g(n+1) = f(g(n)) \ (\forall n \in \mathbb{N})$$

を満たす写像 $g : \mathbb{N} \to S$ が一意的に存在する．

$g(n)$ を a_n と書けば，写像が与えられさえすれば, 数学的帰納法によって数列 $\{a_n\}$ が作れるということだから意味は鮮明だし，胸もすっきりするだろう．証明は付録「集合論のイロハ」を参照．

問題　集合 A から集合 B への全射 $f : A \longrightarrow B$ に対して $f \circ g = \mathrm{idt}_B$($B$ 上の恒等写像) を満たす写像 $g : B \longrightarrow A$ が存在することを選択公理を用いて示せ．

[解答]　$b \in B$ に対して $f^{-1}(b) = A_b$ と置くと $\bigcup_{b \in B} A_b = A$ かつ $A_b \neq \varnothing (\forall b \in B)$ が成り立つ．AC によれば $g : B \longrightarrow \bigcup_{b \in B} A_b$ で $g(b) \in A_b (\forall b \in B)$ を満たすものが存在する．

問題　同値類の代表系の存在を示せ．

[ヒント]　$\widetilde{S} = \{S_a \mid a \in S\}$ と置く．$\widetilde{S}$ は同値類の集合 (商集合) である．S から $\widetilde{S}$ の上への標準的な写像 (すなわち a に S_a を対応させる写像) に対して上の問題の結果を適用せよ．

§2.　選択公理と同値な命題

AC に同値な命題がいくつかあるが，良く知られているのは整列原理，ツォルンの補題である．本節ではこれらを説明しよう．それらの同値性の証明は付録を参照されたい．

§2.1　極大原理 (ツォルンの補題)

代数学では選択公理の同値命題のうち極大原理 (ツォルンの補題) がとりわけ良く使われるので，まずこれについて述べよう．なお，ツォルンの補題と呼ばれることが多いがこれを使ったのはツォルンが最初ではないことに鑑み，本書では極大原理と言うことにする．欧文の本ではこう呼ばれることが多い．

定義　集合 A の元の間に次の 3 条件を満たす関係 $\leqq$ が定義されているとき A は**順序集合**であると言い，$\leqq$ は**順序**であると言われる：

1. $x \leqq x$
2. $x \leqq y \wedge y \leqq x \Longrightarrow x = y$
3. $x \leqq y \wedge y \leqq z \Longrightarrow x \leqq z$

この他にさらに

4. $\forall x \forall y (\in A)\ [x \leqq y \vee y \leqq x]$

すなわち，くだけて言えば A の点が直線上の点のように一列に並んでいるとき A は**全順序集合** (あるいは**線形順序集合**) をなすといわれ，$\leqq$ は A の**全順序** (**線形順序**) であると言われる．

例　集合 S の部分集合の全体のなす集合 (冪集合) を $P(S)$ とする：

$$X \in P(S) \Longleftrightarrow X \subseteqq S$$

$X, Y (\in P(S))$ に対し

$$X \leqq Y \Longleftrightarrow X \subseteqq Y$$

によって関係 $\leqq$ を定義すれば $\leqq$ は $P(S)$ の順序となるが，一般には全順序ではない．

一方, A が $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ のいずれかであれば A には通常の大小関係 $\leqq$ があるがこれが全順序であることは言うまでもない．$\mathbb{C}$ には通常順序を入れない．

定義　順序 $\leqq$ を持った集合 A が**帰納的**順序集合であるとは，A の任意の，全順序をなす部分集合は常に上に有界であることをいう．つまり $B(\subseteqq A)$ が $\leqq$ に関して全順序をなすならば $x \leqq a (\forall x \in B)$ を満たす a $(\in A)$ が存在するとき A は帰納的順序集合と呼ばれるのである．

極大原理　帰納的順序集合は少なくとも一つの極大元を持つ．

記号で書けば，A が帰納的順序集合ならば

$$\exists m\,(\in A)\,\forall x\,(\in A)\,[m \leqq x \Longrightarrow m = x]$$

(m より大きな元は存在しないとき m は極大元と言うのである．)

極大原理を使う代表的な例を問題として挙げておこう．

問題　V を $\mathbb{R}$ 上の (有限次元とは限らない) ベクトル空間とする．V には

基底が存在することを極大原理を用いて証明せよ．

[ヒント]　$\mathbb{R}$ 上 1 次独立な集合 $(\subseteq V)$ の全体のなす集合に包含関係で順序を入れる．

問題　R を環とし，$A(\neq R)$ を R のイデアルとする．このとき $A \subsetneqq M$ なる極大イデアル M が存在することを示せ．

§ 2.2　整列原理

さて，AC に同値な命題である整列原理の説明をするには，整列とはどういうことかを説明しなければならない．

定義　全順序集合 $X = (X, \leqq)$ が**整列集合**であるとは，X の任意の部分集合 $(\neq \varnothing)$ が $\leqq$ に関して最小元を持つときに言われる．

したがって特に X 自身が最小元を有することになる．有限集合ではない最も簡単な整列集合は $\mathbb{N}$ である．$\mathbb{Z}$ も $\mathbb{Q}$ も $\mathbb{R}$ も全順序集合ではあっても整列集合ではない．$\mathbb{Z}$ は，四則演算を自由にできるようにしたという意味で，$\mathbb{N}$ の拡張になっているが，整列性という性質は失ってしまったことになる．$\mathbb{N}$ の持っている整列性 (言い換えれば，数学的帰納法が成立する) という性質を拡張した概念が整列集合である．整列集合の特徴は，数学的帰納法の拡張である超限帰納法が成立することである．

定理 6.2 (超限帰納法の原理)　X を順序 $\leqq$ に関する整列集合とし，$A(x)$ を x に関する命題とする．任意の $x \in X$ に対して

$$\forall y \in X \ (y < x \Longrightarrow A(y)) \Longrightarrow A(x) \tag{2}$$

が成り立つならば，

$$\forall x A(x) \tag{3}$$

が成り立つ．

証明　結論 (3) が成立しないと仮定する．$A(x)$ が成り立たないような $x \in X$ の集合を Y とする：$Y = \{x(\in X) \mid \neg A(x)\}$．すると $X \supseteqq Y \neq \varnothing$ だから，X の整列性によって Y には最小元 y_0 が存在する．つまり $\neg A(y_0)$ であって，$y < y_0$ ならば $A(y)$ が成り立つ．これは (2) に矛盾する．故に (3) が成り立つ．‖

[注意]　$x = x_0$ ($= X$ の最小元) とすると $y < x_0$ なる y は存在しない．つまり (2) の前提部分はないのと同じだから (2) は $A(x_0)$ が成り立つことを仮定していることになる．したがって $X = \mathbb{N}$ の場合は数学的帰納法 (この場合は累積帰納法) と同じである．

超限帰納法が成り立つというのは，簡単に言えば，数学的帰納法の類似がどんな集合に対しても成り立つということだから，大変ありがたい．そこで次の命題が登場する：

整列原理　すべての集合は適当な順序を定義することによって整列集合にすることができる．

この原理を最初に使ったカントルは，これは「思考の法則」であるとした．集合論の基礎に関する議論がカマビスしくなったときツェルメロは選択公理を定式化することによって，整列原理を証明した．この証明の有効性を巡って，ボレル，アダマール，ベール，ルベーグの間で熱い論争が交わされた．これを受けてツェルメロは集合論の公理化に取り掛かることになった．現在の集合論がツェルメロ–フレンケルの集合論 (略して，ZF 集合論) と呼ばれるのには，こういう歴史があるのである．

ついでに言えば，純粋数学というのは，それが矛盾を生じない範囲で理想的状況を設定しておいて，仮定から結論を導く学問であるから，整列原理が正しいかどうか，というようなことは問題にはならない．たとえば，実数体

$\mathbb{R}$ を具体的な順序関係を与えて整列させることは，ZFC 集合論ではできないことがわかっている．しかし，整列できると仮定しても (ZF が矛盾を生じない限り) 何の矛盾も生じないことが重要なのである．現実の物理現象に対する数学の役割 (たとえば電磁気学に微積分学が適用できること) を考えたり，選択公理の役割を考えたりすることは，数学という学問の性格を理解するのに大いに役に立つだろう．選択公理が怪しげだと言うなら，それ以前に自然数の全体 $\mathbb{N}$ を「集合である」と認める方がずっと怪しげである．

さらについでに言えば，数学では「取り出す」,「分ける」,「移す」といった操作に関する言葉を使うが，実際にはそうした操作は行わない (上江洲 [23], pp.176–177 参照)．こうした言葉は，事を明確にするために言い切るなら，数学は物質的であろうと，あるいは理念的であろうと，とにかく実在的対象を取り扱うものだという考え方の名残りである．数学の問題を考えるときには，あたかも実在の対象を触っているかのごとくに考えるのは数学を学ぶ者にとって当然の行為だが，それはいわゆる heuristic (発見的，あるいは教育的) な立場であって，円を二つばかり描いて和集合とか補集合とかを理解するのと五十歩百歩である．客体としての数学はそういうものではない．実在と論理との癒着を引きずっていては，数学の形式としての本質を見誤ることになるだろう．

> 幾何学者たちの使っている言葉は，大変滑稽で無理強いされたようなところがある．というのは彼らはまるで自分たちが実際に行為しているかのように,「正方形にする」とか,「作図する」とか,「加える」というような言い方をするからだ．(プラトン『国家』より)

実際には，これは私が言っていることとは関係の薄い文脈で使われているのだが, 何かとても関係が深いことをプラトンが考えていたように思われて，私には忘れることのできない文章なので引用せずに数学の非操作性を巡る話を終えることができないのである．

定理 6.3　次の三つの命題は同値である (すなわち，ZF 集合論を使って同値が示せる)：

(1)　選択公理

(2)　整列原理

(3)　極大原理 (ツォルンの補題)

証明は付録「集合論のイロハ」を参照せよ．

第7章　代数体へ入門

§1. 2次体

まず一番単純な2次体で肩ならしをしよう．

定理 7.1　m を平方数ではない整数とし，$\theta^2 = m$ なる θ を取る．

$$K = \{x + y\theta \mid x, y \in \mathbb{Q}\}$$

とすると，K は通常の加法・乗法で体をなす．すなわち K は $\mathbb{C}$ の部分体である．

証明　$(x + y\theta) \pm (x' + y'\theta) = (x \pm x') + (y \pm y')\theta$ だから K が加法に関して可換群をなすことは明らかである．

また $(x + y\theta)(x' + y'\theta) = (xx' + myy') + (xy' + x'y)\theta$ であるから結局 K は単位元 $1\ (= 1 + 0\theta)$ を持つ可換環であることがわかった．だからあとは $x + y\theta \neq 0$ すなわち $x = y = 0$ でなければ $\dfrac{1}{x + y\theta} \in K$ であることを言えばよい．

$$\frac{1}{x + y\theta} = \frac{x - y\theta}{x^2 - my^2} = \frac{x}{x^2 - my^2} + \frac{-y}{x^2 - my^2}\theta \in K$$

ここで $x^2 - my^2 \neq 0$ を注意しておこう．‖

高校数学における「分母の有理化」というテクニックがこんなところに顔を出すのである．しかし，たとえば，$1/(3 - \sqrt[3]{2} + \sqrt[3]{4})$ の分母の有理化はど

うやって実現するのだろうかということを考えると，上の証明の最後の部分は $\theta^2 = m$ という特殊性を使っていて一般化がうまくいかないから別証を与えておく．

証明　$f(X) = X^2 - m$ と置くと m は平方数ではないから $f(X)$ は $\mathbb{Q}$ 上既約である．$g(X) = a + bX$ $(a, b \in \mathbb{Q})$ とする．$a = b = 0$ でなければ f と g とは互いに素だから定理 3.5 の系により $\exists h(X), k(X) (\in \mathbb{Q}[X])$；

$$f(X)h(X) + g(X)k(X) = 1$$

$X = \theta$ を代入すると $f(\theta) = 0$ だから $g(\theta)k(\theta) = 1$ を得る．$k(\theta)$ は $\theta^2 = m$ を使って整理すれば K の元であることがわかるから，結局 $g(\theta) = a + b\theta \in K^\times$ には必ず逆元があることになる．‖

この証明だと $f(X)$ が既約でさえあればよいことが見て取れるであろう．割算の原理の威力！　もう一つ割算の原理の威力を見せておこう：

問題　$f(X) \in \mathbb{Q}[X]$ とする．a, b が有理数のとき

$$f(a + bi) = 0 \Longrightarrow f(a - bi) = 0$$

を示せ．

[ヒント]　$g(X) = (X - a - bi)(X - a + bi) = X^2 - 2aX + (a^2 + b^2)$ と置く．$f = qg + r$, $\deg r \leqq 1$ または $r = 0$ と表せば直ちに正解に達する．

もとへ戻ろう．定理 7.1 の K を $\mathbb{Q}(\sqrt{m})$ と書くことにし，有理数体に $\sqrt{m}$ を**添加した**体という．$\mathbb{Q}(\sqrt{m})$ の元は $x + y\sqrt{m}$ $(x, y \in \mathbb{Q})$ とすべて表される．ベクトル空間の言葉で言えば $1, \sqrt{m}$ の $\mathbb{Q}$ 上の 1 次結合で表される．1 と $\sqrt{m}$ とは $\mathbb{Q}$ 上 1 次独立 $(x + y\sqrt{m} = 0 \Longrightarrow x = y = 0)$ だから結局 $\mathbb{Q}(\sqrt{m})$ は $\mathbb{Q}$ 上 2 次元のベクトル空間であることがわかった．$\mathbb{Q}$ 上 2 次元のベクトル空間であるような $\mathbb{C}$ の部分体を ($\mathbb{Q}$ 上の) **2 次体**と呼ぶことにする．

例題　$\mathbb{Q}$ 上の 2 次体 K はすべて

$$K = \mathbb{Q}(\sqrt{m}\,), \quad m \in \mathbb{Z}$$

と表せることを証明せよ．

解答　$\alpha \in K, \alpha \notin \mathbb{Q}$ なる α が存在する．$[K:\mathbb{Q}] = 2$ なので，$1, \alpha, \alpha^2$ は $\mathbb{Q}$ 上 1 次従属だから $\exists a, b, c (\in \mathbb{Q})$；

$$a\alpha^2 + b\alpha + c = 0, \quad (a, b, c) \neq (0, 0, 0)$$

a, b, c の分母の公倍数を両辺にかければ，$a, b, c \in \mathbb{Z}$ と仮定してよいことがわかる．

$a = 0$ ならば $\alpha \in \mathbb{Q}$ となって矛盾するから $a \neq 0$ である．$m = b^2 - 4ac$ と置けば $\alpha \in \mathbb{Q}(\sqrt{m}\,)$．$\mathbb{Q} \subsetneqq \mathbb{Q}(\sqrt{m}\,) \subseteqq K$ かつ K は $\mathbb{Q}$ 上 2 次元だから，$\mathbb{Q}(\sqrt{m}\,) = K$．

$\mathbb{Q}(\sqrt{m}\,)$ は $\mathbb{Z}[\sqrt{m}\,] = \{x + y\sqrt{m} \mid x, y \in \mathbb{Z}\}$ を含む最小の体 (Z の商体) である．それでは $\mathbb{Z}[\sqrt{m}\,]$ の単数とはどんなものだろうか．

問題　$\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}\,]$ に対し $a^2 - b^2m$ を $N(\alpha)$ と記す．次を示せ：

1. $\alpha, \beta \in \mathbb{Z}[\sqrt{m}\,] \Longrightarrow N(\alpha\beta) = N(\alpha)N(\beta)$,
2. αが $\mathbb{Z}[\sqrt{m}\,]$ の単数 $\Longleftrightarrow N(\alpha) = \pm 1$

$\mathbb{Z}[i]$ の単数は $\pm 1, \pm i$ である．また $\mathbb{Z}[\sqrt{-5}\,]$ の単数は ± 1 だけである．

$\mathbb{Z}[\sqrt{-5}\,]$ は $\mathbb{Z}[i]$ に似ているようだが，ある意味では随分違っている．$\mathbb{Z}[i]$ は E.D. だが $\mathbb{Z}[\sqrt{-5}\,]$ はそうでない．P.I.D. でも U.F.D. でもないのである．

$$P = (2, 1 + \sqrt{-5}\,) = \{2x + (1 + \sqrt{-5}\,)y \mid x, y \in \mathbb{Z}[\sqrt{-5}\,]\}$$

とすれば P は $\mathbb{Z}[\sqrt{-5}\,]$ の素イデアルで，単項イデアルではなく $(2) \subsetneqq P$ であることがわかる．(証明は第 9 章にある．) また 6 は $\mathbb{Z}[\sqrt{-5}\,]$ では

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}\,)(1 - \sqrt{-5}\,)$$

と二通りに分解される．しかるに，たとえば 2 が $2=\alpha\beta,\ \alpha,\beta\in\mathbb{Z}[\sqrt{-5}]$，と分解できるとすれば，上の問題より $N(2)=N(\alpha\beta)=N(\alpha)N(\beta)$，$N(2)=4$ だから $N(\alpha)N(\beta)=4$ を得る．α,β が単数 (この場合 ±1) でなければ $N(\alpha)>1, N(\beta)>1 \therefore N(\alpha)=N(\beta)=2$ となりこのような α,β は $\mathbb{Z}[\sqrt{-5}]$ には存在しない．3 や $1\pm\sqrt{-5}$ も同様である．これらの数はこれ以上分解できないけれども $\mathbb{Z}[\sqrt{-5}]$ は P.I.D. ではないから素元というわけにはいかない．$\mathbb{Z}[\sqrt{-5}]$ の性質はこのように $\mathbb{Z}[i]$ とは似ても似つかず複雑である．

§ 2. 代数的数

$\mathbb{Q},\mathbb{C}$ によっていつものように有理数体，複素数体を表すことにする．

定義　$\theta\in\mathbb{C}$ が**代数的数** (algebraic number) であるとは，θ が $\mathbb{Q}$ 上の 1 変数多項式 $(\neq 0)$ の零点になるときにいう：

$$\exists f(X)\in\mathbb{Q}[X];\ f(\theta)=0$$

両辺に適当な整数 $(\neq 0)$ を掛けることによって $f(X)\in\mathbb{Z}[X]$ とすることができることは明らかである．$f(X)\in\mathbb{Q}[X]$ の最高次の係数が 1 のとき $f(X)$ は**モニック**であるということにする：

$$f(X);\ \text{モニック} \iff f(X)=X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n$$

代数的数 θ が整係数モニック多項式の零点となるときに特に**代数的整数** (algebraic integer) であるといわれる：

$$\theta;\ \text{代数的整数} \iff \exists f(X)\in\mathbb{Z}[X];\ f\ \text{はモニック，かつ}\ f(\theta)=0$$

たとえば $\sqrt{2}, \sqrt[3]{2}, i, \dfrac{-1+\sqrt{3}i}{2}$ はすべて代数的整数である．それぞれ，$x^2-2, x^3-2, x^2+1, x^2+x+1$ というモニック整係数多項式の零点となっているからである．またすべての整数は代数的整数である．$m\in\mathbb{Z}$ とすれば m は $X-m$ というモニック整係数多項式の零点だからである．逆に次の定理が成り立つ．

定理 7.2　整数でない有理数は代数的整数でもない．すなわちすべての代数的整数の全体を $\mathbb{O}$ と記せば，

$$\mathbb{O} \cap \mathbb{Q} = \mathbb{Z}$$

が成り立つ．

証明　$q/p, (p,q) = 1$ を有理数とする．q/p がモニック整係数多項式 $f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n, a_j \in \mathbb{Z} (j = 1, 2, \cdots, n)$ の零点であるとする．

$$\left(\frac{q}{p}\right)^n + a_1 \left(\frac{q}{p}\right)^{n-1} + \cdots + a_{n-1} \left(\frac{q}{p}\right) + a_n = 0$$

$\therefore\ q^n = -p\left(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_{n-1} p^{n-2} q + a_n p^{n-1}\right)$ $\ \therefore\ p | q^n$．ところが $(p,q) = 1$ だから $p = \pm 1$．故に q/p は有理整数である．∥

かくして代数的整数は整数という概念の拡張であることがわかった．だから整数論の世界では，普通の整数のことを**有理整数**と呼んで区別を明確にすることも行われている．次の定理はよく知られている：

定理 7.3 (ガウスの補題)　係数の最大公約数が 1 であるような整係数多項式は**原始的**であると言われる．しからば原始多項式の積は原始多項式である．

証明

$$f(X) = \sum_{i=0}^{m} a_i X^i, \quad g(X) = \sum_{j=0}^{n} b_j X^j \quad (a_i, b_j \in \mathbb{Z})$$

が共に原始的であるとする：

$$(a_0, \cdots, a_m) = 1, \quad (b_0, \cdots, b_n) = 1$$

p を素数とする．$p|a_0, \cdots, p|a_{r-1}$ だが $p \nmid a_r$ なる r と $p|b_0, \cdots, p|b_{s-1}$ だが $p \nmid b_s$ なる s を取る．$f(X)g(X)$ における X^{r+s} の係数は $\sum_{i+j=r+s} a_i b_j$ である．容易にわかるように $a_r b_s$ 以外の項は r, s の選び方から p で割れる：

$$\sum_{i+j=r+s} a_i b_j \equiv a_r b_s \pmod{p}$$

$a_r b_s \not\equiv 0 \pmod{p}$ であるから X^{r+s} の係数は p で割れない．どの素数についてもそうだから $f \cdot g$ は原始的であることが示されたことになる．∥

ガウスの補題の証明の応用例として，次の定理の証明をしておこう．

定理 7.4　R が U.F.D. ならば $R[X]$ も U.F.D. である．

証明　1. まず R の素元は $R[X]$ においても素元であることを示す．p を R の素元とする．$p \nmid F(X)$, $p \nmid G(X)$ ならば $p \nmid F(X)G(X)$ を示せばよいが，その証明はガウスの補題の証明とまったく同じである．

2. 次に，$R[X]$ の既約な原始多項式は $R[X]$ の素元であることを示す．

$\varphi(X) \in R[X]$ を既約な原始多項式とし，$\varphi(X)|F(X)G(X)$ とする $(F, G \in R[X])$．R は整域だからその商体 K を作ることができる．$K[X]$ はユークリッド環だから U.F.D. である．しかも $\varphi(X)$ が $K[X]$ の既約元であることは容易にわかるから，素元でもあることになる．たとえば $\varphi(X)|F(X)$ とすると $F(X) = \varphi(X)f(X), f(X) \in K[X]$ と書ける．そこで

$$F(X) = a\psi(X), \quad f(X) = \frac{c}{b}\xi(X) \quad (a, b, c \in R)$$

となるような原始多項式 $\psi(X), \xi(X)$ を取ると

$$ab\psi(X) = c\varphi(X)\xi(X)$$

を得るが，$\varphi(X)\xi(X)$ も原始多項式だから，両辺を展開して係数の最大公約数を考えれば $ab = c$ がわかる．したがって $c/b = a \in R$ であって，$f(X) \in R[X]$ を得る．つまり $R[X]$ において $\varphi(X)|F(X)$ である．

3. さて $F(X) \in R[X]$ としよう．

$$F(X) = aG(X), \quad G(X) \text{ は原始的}, \quad a \in R$$

と表す．a を R で素元分解すれば，それはそのまま $R[X]$ での a の素元分解である．次に $G(X)$ を $K[X]$ の元とみて素元分解する：

$$G(X) = F_1(X) \cdots F_s(X)$$

$F_i(X)$ を $\dfrac{b_i}{a_i}f_i(X)$, $f_i \in R[X]$ は原始的，また $a_i, b_i \in R$ と表すと $f_i(X)$ は既約元，すなわち素元であって，

$$aG(X) = bf_1(X) \cdots f_s(X), \quad a, b \in R$$

となる．先と同じ議論によって $a = b$ を得る．$G(X) = f_1(X) \cdots f_s(X)$ は $R[X]$ における素元分解である．一意性の証明は容易である．‖

θ が代数的整数であるとは θ の満たす方程式の中にモニックで整係数のものがあることだったが，実は θ の満たす既約方程式もモニック整としてよいことを証明する．これは定理 7.2 の拡張である．

定理 7.5 θ が代数的整数であるとすると，θ が零点となる既約原始多項式はモニックである．

証明 定義よりモニック整係数多項式 $f(X)$ で $f(\theta)=0$ となるものが存在する．$g(X)$ を $g(\theta)=0$ なる既約原始多項式とする．$g(X)$ の既約性から $g|f$ が割算の原理を用いて証明される．すなわち $\exists h(X)\in\mathbb{Q}[X]$;

$$f(X)=g(X)h(X).$$

定理 7.4 の証明と同様にして $h(X)\in\mathbb{Z}[X]$ で，しかも原始的としてよいことがわかる．$f(X)$ はモニックだから，$g(X)$ は最高次の係数が ± 1 でなくてはならない．すなわち本質的にはモニックである．‖

次の定理はデデキントによるものだが，授業で証明を話すたびに，その簡明さと鮮やかさに感銘を覚える．

定理 7.6 代数的数の全体 $\overline{\mathbb{Q}}$ は体をなす．代数的整数の全体 $\mathbb{O}$ は環をなす．

証明 まず $\alpha,\beta\in\mathbb{O}\Longrightarrow\alpha+\beta\in\mathbb{O}$ を証明する．α,β は代数的整数なので，ある自然数 m,n を取ると

$$\alpha^m=a_1\alpha^{m-1}+\cdots+a_{m-2}\alpha+a_{m-1},\ a_i\in\mathbb{Z}$$
$$\beta^n=b_1\beta^{n-1}+\cdots+b_{n-2}\beta+b_{n-1},\ b_j\in\mathbb{Z}$$

と表せる．そこで mn 個の数

$$\alpha^i\beta^j\ (i=0,1,\cdots,m-1;j=0,1,\cdots,n-1)$$

を適当に並べて

$$\omega_1,\cdots,\omega_N\quad(N=mn)$$

と書くことにする．$\gamma = \alpha + \beta$ と置くと $k(1 \leqq k \leqq N)$ に対して

$$\gamma\omega_k = c_{k1}\omega_1 + \cdots + c_{kN}\omega_N \ (c_{kj} \in \mathbb{Z})$$

と書ける．(たとえば $\omega_k = \alpha$ とすると $\alpha \cdot \alpha^i\beta^j = \alpha^{i+1}\beta^j$ で，$i+1 < m$ なら，これはいずれかの $\omega_{k'}$ であるし，$i+1 = m$ ならより次数の低い項の和として表せるからである.) 以上より

$$\begin{cases} (c_{11} - \gamma)\omega_1 + c_{12}\omega_2 + \cdots + c_{1N}w_N = 0 \\ c_{21}\omega_1 + (c_{22} - \gamma)\omega_2 + \cdots + c_{2N}\omega_N = 0 \\ \qquad\qquad \cdots \qquad \cdots \\ c_{N1}\omega_1 + c_{N2}\omega_2 + \cdots + (c_{NN} - \gamma)\omega_N = 0. \end{cases}$$

この式を $\omega_1, \cdots, \omega_N$ の連立 1 次方程式とみると非自明解の存在するための条件として

$$\begin{vmatrix} c_{11} - \gamma & c_{12} & \cdots & c_{1N} \\ c_{21} & c_{22} - \gamma & \cdots & c_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N1} & c_{N2} & \cdots & c_{NN} - \gamma \end{vmatrix} = 0$$

が得られる．これを展開すれば γ の満たす N 次式が得られ γ_N の係数は ± 1，他の係数は整数である故，γ は代数的整数である．積 $\alpha\beta$ についても同様．同時に α, β がそれぞれ m 次，n 次の方程式の根であれば $\alpha + \beta$, $\alpha\beta$ は mn 次方程式を満たすことも知られる．

以上によって $\mathbb{O}$ は環をなすことが証明された．$\overline{\mathbb{Q}}$ が体をなすことを知るには $\overline{\mathbb{Q}} \ni \alpha (\neq 0)$ ならば $\alpha^{-1} \in \overline{\mathbb{Q}}$ であることを示せばよい．しかしこれは α の満たす m 次方程式が与えられれば，両辺を α^m で割って α^{-1} の満たす方程式が得られることから明らかである．‖

問題　$\theta \in \overline{\mathbb{Q}} \Longrightarrow \exists a\ (\neq 0) \in \mathbb{Z}; a\theta \in \mathbb{O}$ を証明せよ．

定理 7.7　K を $\mathbb{C}$ の部分体とし，$\theta\ (\in \mathbb{C})$ は K 上 n 次の既約多項式の零

点であるとする：

$$\exists f(X) \in K[X]; f(X) \text{ は既約}, \ \deg f = n, \ f(\theta) = 0$$

すると K と θ を含む $\mathbb{C}$ の最小の部分体 $K(\theta)$ は

$$K(\theta) = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \cdots, a_{n-1} \in K\}$$

と表せる．

[注意]　上式の右辺は K と θ とを含む最小の環であって，普通 $K[\theta]$ と表される．左辺の $k(\theta)$ は K と θ を含む最小の体を意味する記号であるから，定理は $K(\theta) = K[\theta]$ を主張しているのである．たとえば円周率 π は代数的数ではないから $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$ である．左辺は分母・分子が π の多項式の集合，右辺は π の多項式の集合だからである．

証明　2 次体のときと同じである．右辺が環をなすことは明らかだから，$g(\theta) = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ $(\neq 0)$ は常に逆元を持つことを言えばよい．$g(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ とする．$(f, g) = 1$ であるから割算の原理によって

$$fp + gq = 1$$

を満たす $p(X), q(X)$ $(\in K[X])$ が存在する．両辺に θ を代入して $f(\theta) = 0$ を用いれば $g(\theta)q(\theta) = 1$ が得られる．そこで $q(\theta)$ を $b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}$ $(b_0, b_1, \cdots, b_{n-1} \in K)$ の形に表せばよい．‖

§ 3. 代数体とその整数環

L を体 K の拡大体とする．(この状況のとき L/K と記す.) すなわち，集合として $K \subsetneqq L$ であり，L の加法・乗法を K に制限すると K の加法・乗法となるのである．このとき L は K 上のベクトル空間とみなせる．なぜなら $a, b \in K$, $\alpha, \beta \in L$ とすれば

$$a(\alpha + \beta) = a\alpha + a\beta, \ (a + b)\alpha = a\alpha + b\alpha,$$
$$(ab)\alpha = a(b\alpha), \ 1 \cdot \alpha = \alpha$$

などのベクトル空間の公理系が満たされるからである．

K 上のベクトル空間とみたときの L の K 上の次元のことを L の K 上 (あるいは L/K) の**拡大次数**といって，それを表すのに

$$[L:K]$$

という記号を充てる．

たとえば 2 次体 $\mathbb{Q}(\sqrt{2})$ の場合は $1, \sqrt{2}$ が $\mathbb{Q}$ 上 $\mathbb{Q}(\sqrt{2})$ の基底となる．なぜならば，任意の $\alpha \in \mathbb{Q}(\sqrt{2})$ は

$$\alpha = a + b\sqrt{2} \quad (a, b \in \mathbb{Q})$$

と表せるし，

$$x + y\sqrt{2} = 0 \quad (x, y \in \mathbb{Q}) \Longrightarrow x = y = 0 (1 \text{ 次独立性})$$

が成り立つからである．故に

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

である．同様に，一般に L/K が 2 次体なら

$$[L:K] = 2$$

である．

問題　$L = K(\theta)$，ここに θ は K 係数の n 次既約多項式の零点，とすれば，

$$[L:K] = n$$

が成り立つ．これを証明せよ．

[ヒント]　$\{1, \theta, \cdots, \theta^{n-1}\}$ が L の K 上の基底をなす．

定義　K を $\mathbb{C}$ の部分体 (つまり，$\mathbb{C}$ は K の拡大体) とする．$[K:\mathbb{Q}] < \infty$，すなわち体 K が有理数体上の有限次元のベクトル空間であるとき，K は**有限次代数体**，略して**代数体**と呼ばれる．

定理 7.8 (原始要素の存在)　L/K を代数体の拡大とすると，適当な代数的数 θ を用いて $L = K(\theta)$ と表せる．

証明　$[L:K]=n$ とすれば，拡大次数の定義から

$$L = K\theta_1 + \cdots + K\theta_n = \{a_1\theta_1 + \cdots + a_n\theta_n \mid a_1, \cdots, a_n \in K\}$$

となる $\theta_1, \cdots, \theta_n$ $(\in L)$ が存在する．したがって特に

$$L = K(\theta_1, \cdots, \theta_n) \ (= K, \theta_1, \cdots, \theta_n \text{ を含む最小の代数体})$$

である．故に $L = K(\xi, \eta)$ のとき $L = K(\theta)$ となる θ が取れることを示せば定理の証明が終わる．

ξ, η の満たす K 上のモニック既約多項式を $f(X), g(X)$ とし，その零点をそれぞれ $\xi_1(=\xi), \cdots, \xi_m$ と $\eta_1(=\eta), \cdots, \eta_n$ としよう．すると，

$$f(X) = (X-\xi_1)\cdots(X-\xi_m)$$

である．そこで $c \in K$ を

$$\zeta_{ij} = c\xi_i + \eta_j \quad (i = 1, \cdots, m; j = 1, \cdots, n)$$

がすべて異なるように取る．これは K には無数の元があるから可能である．

$$h(X) = g(\zeta_{11} - cX) \in K(\zeta_{11})[X]$$

と置けば

$$h(\xi_1) = 0, \quad h(\xi_i) \neq 0 \quad (i \neq 1)$$

が成り立つ．したがって $X - \xi_1$ は $f(X)$ と $h(X)$ の G.C.D.(最大公約多項式) となる．G.C.D. は互除法によって得られるから $f(X), h(X) \in K(\zeta_{11})[X]$ によって $X - \xi_1 \in K(\zeta_{11})$．故に $\eta_1 = \zeta_{11} - c\xi_1 \in K(\zeta_{11})$ を得る．

$$\therefore \quad L \subsetneqq K(\zeta_{11}).$$

一方，$\zeta_{11} = c\xi_1 + \eta_1 \in L$ だから $L = K(\zeta_{11})$ が得られる．‖

例えば $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ としよう．$\theta = \sqrt{2} + \sqrt{3}$ と置けば，上の定理の証明から $L = \mathbb{Q}(\theta)$ であることがわかる．

代数体 K に属する代数的整数の全体を $\mathbb{O}_K$ と記せば $\mathbb{O}_K = \mathbb{O} \cap K$ で $\mathbb{O}, K$ は共に環なのだから $\mathbb{O}_K$ も環をなす，すなわち加法・減法・乗法で閉じている．$\mathbb{O}_K$ を K の**整数環**という．

§ 4.　共役体

K を代数体とする．K からすべての代数的数のなす体 $\overline{\mathbb{Q}}$ への準同型写像 $\sigma : K \longrightarrow \overline{\mathbb{Q}}$ のことを K の**共役写像**と言う．条件を具体的に書けば

$$\sigma(x+y) = \sigma(x) + \sigma(y), \quad \sigma(xy) = \sigma(x)\sigma(y)$$

が成り立つとき K の共役写像と言うのであるが，$\sigma(x) = 0$ $(\forall x \in K)$ という零写像は除外して考えるので，実際には共役写像は単射である．何故なら σ の核 $\sigma^{-1}(0)$ は K のイデアルだが，K にはイデアルは $(0) = \{0\}$ と $(1) = K$ しか存在せず，後者は除外されているからである．このような場合 (つまり，単射準同型の場合) は「中への同型写像」という言い方をすることが多い．

さて，$\mathbb{Q}(\theta)$ となる θ を取り，θ の満たす既約多項式 $f(X) (\in \mathbb{Q}[X])$ を取る．$f(X) = 0$ はすべての代数的数のなす体 $\overline{\mathbb{Q}}$ において $n(= \deg f)$ 個の解を有する．それを

$$\theta^{(1)}(=\theta),\ \theta^{(2)}, \cdots, \theta^{(n)}$$

と番号付けよう．σ を K の共役写像とすれば $\sigma(\theta) = \theta^{(j)}$ となる j が存在する．何故なら

$$f(\theta) = a_0 + a_1\theta + \cdots + a_n\theta^n = 0 \quad (a_0, a_1, \cdots, a_n \in \mathbb{Q})$$

に σ をほどこせば

$$a_0 + a_1\sigma(\theta) + \cdots + a_n(\sigma(\theta))^n = 0$$

を得るからである．($\sigma(1) = 1$ により σ は必然的に $\mathbb{Q}$ の元 a に対して $\sigma(a) = a$ を満たすことに注意.)

したがって，共役写像 σ は具体的には

$$\sigma\left(\sum_{i=0}^{n-1} a_i\theta^i\right) = \sum_{i=0}^{n-1} a_i(\theta^{(j)})^i$$

という作用によって与えられるのである．逆に θ の共役数 $\theta^{(j)}$ を任意に一つ選ぶと，

$$K = \mathbb{Q}(\theta) \simeq \mathbb{Q}(\theta^{(j)}) \subseteq \overline{\mathbb{Q}}$$

となって，共役写像が得られる．実際，

$$\begin{array}{ccccc}
\mathbb{Q}(\theta) & \simeq & \mathbb{Q}[X]/(f(X)) & \simeq & \mathbb{Q}(\theta^{(j)}) \\
\Psi & & \Psi & & \Psi \\
\sum_{i=0}^{n-1} a_i\theta^i & \longleftrightarrow & \sum_{i=0}^{n-1} a_i X^i \bmod f(X) & \longleftrightarrow & \sum_{i=0}^{n-1} a_i(\theta^{(j)})^i
\end{array}$$

によって同型写像が与えられるのである．

以上を要約すれば，K の中への共役写像とは $K = \mathbb{Q}(\theta)$ なる θ に共役数 $\theta^{(j)}$ を対応させることから誘導される写像 $\mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta^{(j)}) \subsetneqq \overline{\mathbb{Q}}$ のことである．したがって共役写像は n 個存在する．

なお共役写像は n 個あるが，K の共役体 $K^{(j)} = \mathbb{Q}(\theta^{(j)})$ は n 個あるとは限らない，つまり $K^{(1)}, \cdots, K^{(n)}$ がすべて異なる集合であるとは限らない．例えば $K = \mathbb{Q}(\sqrt{2})$ とすれば $\sqrt{2}$ の共役数は $\pm\sqrt{2}$ であるので，共役写像は $x + y\sqrt{2} \longrightarrow x + y\sqrt{2}$ と $x + y\sqrt{2} \longrightarrow x - y\sqrt{2}$ の二つあるけれども，$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ だから $\mathbb{Q}(\sqrt{2})$ の共役体はそれ自身しか存在しない．

§ 5. 群の同型

代数的整数論は代数体の整数環の理論なのだが，ガロア理論など群論を利用することが多い．ここで群について一歩考察を進めておく．

定義　G, G' を群とする．写像 $f : G \longrightarrow G'$ は条件

$$f(xy) = f(x)f(y)$$

を満たすとき**準同型写像** (homomorphism) であると言われる．さらに f が 1 対 1，上への写像であれば**同型写像** (isomorphism) と呼ばれる．同型写像が存在するような群は互いに**同型**である (isomorphic) といわれ，$G \simeq G'$ と記される．

例　$\mathbb{R}$ を加法だけに注目してアーベル群とみなす．また，$\mathbb{R}^+ = \{x\ (\in \mathbb{R}) \mid x > 0\}$ は乗法群をなす．$f : \mathbb{R} \longrightarrow \mathbb{R}^+$ を $f(x) = e^x$ で定義する．

$$f(x + y) = f(x)f(y)$$

が成り立ち，しかも $f(x) = f(y)$ より $x = y$ が得られるから 1 対 1，$\forall y \in \mathbb{R}^+$ に対し $f(\log y) = y, \log y \in \mathbb{R}$ だから上への写像，すなわち同型写像である．

例　G を群，N を G の正規部分群，すなわち $xN = Nx\ (\forall x \in G)$ が成り立つとする．xN を $\overline{x}$ と記そう．しからば，

$$\varphi : G \longrightarrow G/N, \quad ここに \quad \varphi(x) = xN = \overline{x}$$

は上への準同型写像である．これは $\overline{x} \cdot \overline{y} = \overline{xy}$ が成り立つからである．φ は**自然準同型写像**と呼ばれる．

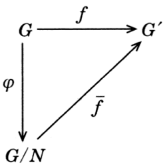
問題　$f : G \longrightarrow G'$ を群の準同型写像とし，e, e' を G, G' の単位元とする．次を示せ：

1. $N = \{x\ (\in G) \mid f(x) = e'\}$($f$ の**核**) は G の正規部分群である．
2. $f(G) = \{f(x) \mid x \in G\}$($f$ の**像**) は G' の部分群をなす．
3. $f(e) = e'$.
4. $f(x)^{-1} = f(x^{-1})$.
5. f が 1 対 1 であるためには $f(x) = e' \Longrightarrow x = e$ であることが必要十分である．

定理 7.9 (群の準同型定理)　$f : G \longrightarrow G'$ を群 G から群 G' の上への準同型写像とする．N を f の核，すなわち $N = \{x\ (\in G) \mid f(x) = e'\}$ とすれば，次の図式が可換となるような同型写像 $\overline{f} : G/N \longrightarrow N'$ が存在する：すなわち $f = \overline{f} \cdot \varphi$，ここで φ は自然準同型写像とする．

証明　$\overline{f}(\overline{x}) = f(x)$ と定義する．これは x の属する類の行先を x の f による行先と定めることである．だからまず $\overline{x} = \overline{y}$ ならば $f(x) = f(y)$ なること，すなわち $\overline{f}$ は well defined なること (合理的に定義されていること) を示さねばならない．

$\overline{x} = \overline{y}$ ならば N による類別の定義から



$$\exists z \in N; y = zx$$
$$\therefore \quad f(y) = f(zx) = f(z)f(x) = e'f(x) = f(x)$$
$$\therefore \quad f(x) = f(y)$$

ここで f が準同型写像なること，$z \in N$ だから $f(z) = e'$，そして e' は G' の単位元であることを使った．

$\overline{f}$ が準同型写像であること：

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$$

$\overline{f}$ が 1 対 1 であること：

$$\overline{f}(\overline{x}) = e' \Longrightarrow \overline{x} = \overline{e} \ (= G/N \text{ の単位元})$$

を示せばよい．

$\overline{f}(\overline{x}) = e'$ より $f(x) = e'$． $\therefore \quad x \in N \quad \therefore \quad \overline{x} = \overline{e}$

$\overline{f}$ が上への写像であること：$\forall x' \in G'$ を取る．f が上への写像だから

$$\exists x \ (\in G); f(x) = x' \quad \therefore \quad \overline{f}(\overline{x}) = x'$$

図式の可換性の証明：

$$(\overline{f} \cdot \varphi)(x) = \overline{f}(\varphi(x)) = \overline{f}(\overline{x}) = f(x) \quad \therefore \quad \overline{f} \cdot \varphi = f \quad \|$$

この定理は群の同型性を証明する際に基本となる大切な定理である．

系 1　N_1, N_2 が G の正規部分群で，$N_2 \subsetneqq N_1$ ならば，

$$(G/N_2) / (N_1/N_2) \simeq G/N_1$$

証明　$f : G/N_2 \longrightarrow G/N_1$ を

$$f(xN_2) = xN_1$$

で定義する．f が上への準同型写像であることはほぼ明らか．$f(xN_2) = eN_1$ ならば $xN_1 = eN_1$，すなわち $x \in N_1$．故に単位元 $eN_1 = N_1$ に写像される元の全体は N_1/N_2 である．準同型定理により証明終わり．∥

系 2　H を G の部分群，N を G の正規部分群とすれば，

$$H/(N \cap H) \simeq HN/N$$

問題　系 2 を証明せよ．

[ヒント]　$f : H \longrightarrow HN/N$ を $f(x) = xN$ で定義し，準同型定理を適用する．

例題　G を巡回群とする．次を証明せよ：

1. G の位数が無限ならば $G \simeq \mathbb{Z}$
2. G の位数が n ならば $G \simeq \mathbb{Z}/n\mathbb{Z}$

[注意]　$\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ は共に環であるから当然 $+$ に関して群 (加群) をなす．その加群としての構造に注目しているのである．これが「群として同型」の意味である．$\mathbb{Z}$ の生成元は 1(あるいは -1) で他のすべての元は 1 のいくつかの和およびその加法逆元として表される．また $\overline{1}$ (あるいは $\overline{-1}$) は $\mathbb{Z}/n\mathbb{Z}$ の生成元である．

証明　G の生成元を s とする：

$$G = \{s^n \mid n \in \mathbb{Z}\}$$

写像 $f : \mathbb{Z} \longrightarrow G$ を $f(n) = s^n$ で定義する．

$$f(m+n) = s^{m+n} = s^m \cdot s^n = f(m)f(n)$$

だから f は加群 $\mathbb{Z}$ から群 G への準同型写像である．明らかに全射であるか

ら準同型定理が適用できる．

$N = \{n \in \mathbb{Z} \mid f(n) = e\ (= s^0)\}$ と置く．G の位数が無限ならばどの $n\ (\neq 0)$ に対しても $s^n \neq e$ だから $N = \{0\}$．このとき $G \simeq \mathbb{Z}$.

G の位数が有限で n ならば

$$s^m = e \Longleftrightarrow n|m \Longleftrightarrow m \in (n)$$
$$\therefore\quad N = (n) \quad\therefore\quad G \simeq \mathbb{Z}/n\mathbb{Z} \quad \|$$

G_1, G_2 を群とし，直積 $G_1 \times G_2$ を考える：

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1,\ x_2 \in G_2\}$$

$x = (x_1, x_2) \in G_1 \times G_2$，$y = (y_1, y_2) \in G_1 \times G_2$ に対し，

$$xy = (x_1 y_1, x_2 y_2)$$

によって積を定義する．すなわち成分同士かけ合わせるのだ．

問題　この積の定義で $G_1 \times G_2$ は群をなすことを示せ．

問題　N_1, N_2 を G_1, G_2 の正規部分群とすると

$$(G_1 \times G_2) / (N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2)$$

が成り立つ．これを準同型定理から証明せよ．

[ヒント]　$f : G_1 \times G_2 \longrightarrow (G_1/N_1) \times (G_2/N_2)$ を自然な方法で定義し，定理 7.9 を適用する．

G_1, G_2 が**加群** (すなわち演算が $+$ で記されたアーベル群) であれば直積は**直和**とよばれ，

$$G_1 \oplus G_2$$

と記される：

$$(x_1, x_2) + (y_1, y_2) \overset{\text{定義}}{=} (x_1 + y_1, x_2 + y_2)$$

n 個の群 $G_1, \cdots, G_n$ の直積および直和の定義も同様にして行われる．

さて群 G が**有限生成**であるというのは G が有限個の元から生成されるということ，すなわち適当な $s_1, \cdots, s_n\ (\in G)$ を選ぶと $s_1, \cdots, s_n$ を含む G の最小の部分群が G そのものになる場合を言う．このとき $\{s_1, \cdots, s_n\}$ は G の**生成系**であると言われる．G が有限生成の群であるとは有限集合の生成系を有することと言い換えられる．

巡回群はただ一つの元から生成されるから最も単純な有限生成の群である．

有限生成ではないアーベル群もいくらでもある．たとえば，正の有理数の全体のなす乗法群 G を考えてみよう．すべての素数の集合を P とすると，G は有限生成ではないが，G の元は

$$\prod_{p\in P} p^{n_p}$$

(ここに n_p は整数で，有限個を除けば 0 とする) という形に一意的に表せるので，G は基底 P を持つアーベル群であると表現することができる．しかし，正の実数の全体のなす乗法群は P のような基底を持っていない．群論的に見ても，有理数体と実数体はこんなに違うのである．

§ 6.　環の同型

群の準同型定理を述べたから，同じ思想圏にある概念として，ここで環の準同型定理を述べるのは，前節の前半部分を逐語的に繰り返すのみで済むので，時宜を得ているだろう．

定義　R, R' を環 (単位元を有する可換環) とする．写像 $f : R \longrightarrow G'$ は条件

$$f(x+y) = f(x) + f(y),\ f(xy) = f(x)f(y)$$

を満たすとき**準同型写像** (homomorphism) であると言われる．さらに f が 1 対 1，上への写像であれば**同型写像** (isomorphism) と呼ばれる．同型写像が存在するような環は互いに**同型**である (isomorphic) と言われ，$R \simeq R'$ と記される．

例　R を環，A を R のイデアル $(\neq R)$ とする．$x+A\ (=\{y\ (\in R) \mid y-x\in A\})$ を $\overline{x}$ とも $x \bmod A$ とも記そう．しからば，

$$\varphi : R \longrightarrow R/A, \quad ここに \varphi(x) = x \bmod A$$

は上への準同型写像である．これは

$$\varphi(x+y) = \varphi(x)+\varphi(y), \quad \varphi(xy) = \varphi(x)\varphi(y)$$

が成り立つからである．φ は**自然準同型写像**と呼ばれる．

問題　$f : R \longrightarrow R'$ を環の準同型写像とし，$0, 0'$ を R, R' の加法単位元とする．次を示せ：

1. $A = \{x\ (\in R) \mid f(x) = 0'\}$($f$ の**核**) は R のイデアルである．
2. $f(R) = \{f(x) \mid x \in R\}$($f$ の**像**) は R' の部分環をなす．
3. $f(0) = 0'$.
4. $f(-x) = -f(x)$.
5. f が 1 対 1 であるためには $f(x) = 0' \Longrightarrow x = 0$ が必要十分である．

定理 7.10 (環の準同型定理)　$f : R \longrightarrow R'$ を環 R から環 R' の上への準同型写像とする．A を f の核，すなわち $A = \{x\ (\in R) \mid f(x) = 0'\}$ とすれば，$f = \overline{f}\cdot\varphi$ となるような同型写像 $\overline{f} : R/A \longrightarrow R'$ が存在する．ここで $\varphi : R \longrightarrow R/A$ は自然準同型写像とする．

証明も群の準同型定理を逐語的に追えばよいから，読者に任せよう．

第8章　有限生成アーベル群の基本定理

§1. 証明の前に応用例を

有限生成アーベル群の基本定理　有限生成アーベル群 G は有限個の巡回群の直積に同型である．詳しく言うと，

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_s)$$

ここに $\mathbb{Z}^r = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$($r$ 個の直和) かつ $n_j | n_{j+1} (j = 1, \cdots, s-1)$ と分解できて，しかも r, s および $n_1, \cdots, n_s (n_j > 1)$ は G によって一意に定まる．

この定理の証明は次章で与える．整数環，単数群など代数的整数論では加群がしばしば扱われるから有限生成アーベル群の基本定理は整数論の土台を支える代数学の定理と言うことができる．

命題　G_1, G_2 をそれぞれ位数 m_1, m_2，ただし $(m_1, m_2) = 1$ の巡回群とすれば，直積 $G_1 \times G_2$ は位数 $m_1 m_2$ の巡回群である．

証明　仮定によって，

$$G_1 \simeq \mathbb{Z}/m_1\mathbb{Z}, \quad G_2 \simeq \mathbb{Z}/m_2\mathbb{Z}$$

である．$(m_1, m_2) = 1$ だから定理 2.3 によって

$$\mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \simeq \mathbb{Z}/m_1 m_2\mathbb{Z}$$

が成り立つ．なお，定理 2.3 は写像の全単射性のみを述べているが，この写像が環としての，したがって当然加群としての，同型性を有することは明らかである．念のため，写像を復習しておくなら，

$$x \bmod m_1m_2 \rightsquigarrow (x \bmod m_1,\ x \bmod m_2)$$

である．ここに $a \rightsquigarrow b$ は a に b を対応させるという意味である．‖

この命題を逆に見れば，G が位数 m_1m_2 の巡回群であって $(m_1, m_2) = 1$ ならば，G は位数がそれぞれ m_1, m_2 の巡回群 G_1, G_2 の直積として表せるということである．

この命題と有限生成アーベル群の基本定理を組み合わせて容易に次の定理を得る．その前に定義を一つ．

定義　p を素数とする．位数が p の冪なる有限群 G は p 群と呼ばれる．

定理 8.1　1. 有限アーベル群 G を

$$G \simeq G_1 \times \cdots \times G_n$$
$$\text{ここに } G_j \text{は } p_j \text{群 } (p_1, \cdots, p_n \text{は相異なる素数})$$

と直積分解することが可能である．

2. G が有限アーベル p 群であれば

$$G \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_s}\mathbb{Z},$$
$$1 \leqq n_1 \leqq n_2 \leqq \cdots \leqq n_s$$

と一意的に分解できる．

同じ G の分解を $\times$ (直積) で表してみたり $\oplus$ (直和) で表してみたり，初めのうちは奇妙に感じるかもしれない．しかし本質的にはどちらで書こうとまったく変わりはない．要するに慣れの問題であるからその場その場で都合の良い方を使えばよい．

系　G を有限アーベル群とする．G が巡回群であるためには，任意の素数 p に対して G における方程式

$$x^p = e \quad (G\text{ の単位元}) \tag{1}$$

が p 個以内の解を持つことが必要十分である．

証明 (系の証明)　G を巡回群とし，生成元を g，位数を n とする．$x = g^j$ と置くと (1) から $g^{pj} = e$.　$\therefore$ $pj \equiv 0 \pmod n$. $p|n$ ならば $j \equiv 0 \pmod m$，ここに $m = n/p$. 故に (1) の解は $g^m, g^{2m}, \cdots, g^{(p-1)m}, g^{pm} = e$ の p 個である．$p \nmid n$ ならば $pj \equiv 0 \pmod n$ から $j \equiv 0 \pmod n$ を得る．故に (1) の解は e だけである．

次に G が巡回群ではないとしよう．有限生成アーベル群の基本定理によって

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_s\mathbb{Z},\ n_j|n_{j+1} \quad j = 1, 2, \cdots, s-1, \quad n_1 > 1$$

と分解できる．G が巡回群でないことから $s > 1$.

n_1 を割り切る素数を一つ取って p とする：$p|n_1$. すると $p|n_j$ でもある ($\because$ $n_1|n_j$). しからば (1) は G において p^s 個の解を有する．これは各 $\mathbb{Z}/n_j\mathbb{Z}$ においては $px \equiv 0 \pmod{n_j}$ は $p|n_j$ によって p 個の解を有することから明らかである．‖

なお，G を割り切る素数についてだけ調べればよいことは明らかである．とくにアーベル p 群であれば，その p に対してだけ方程式 (1) が p 個の解を持つことを知れば G は巡回群であることが結論できる．

定理 8.2　F を (可換) 体とする．M が乗法群 $F^\times = \{a\ (\in F) \mid a \neq 0\}$ の有限部分群であれば M は実は巡回群である．

証明　p を任意の素数とし，F における方程式

$$x^p = 1 \quad (F\text{ の乗法単位元}) \tag{2}$$

を考察する．F は体であるから (2) は F 内に高々 p 個の解しか有しない．

(第 3 章, p.50 の最後の問題参照.) したがって M に属する解も高々 p 個である. 定理 8.1 の系によれば, これは M が巡回群であることを示している. ‖

系　F を有限体とすれば $F^{\times}$ は巡回群である. したがって特に p を法とする既約剰余類群 $(\mathbb{Z}/p\mathbb{Z})^{\times}$ は巡回群である.

この系はガウス ([5]) によって証明された有名な定理である. $a \bmod p$ が $(\mathbb{Z}/p\mathbb{Z})^{\times}$ の生成元となるとき, 整数 a は法 p の**原始根**であると歴史的に言い慣わしている.

体と言えばわれわれは可換体, すなわち乗法については可換法則

$$ab = ba$$

が満たされる体だけを扱っているのだった. しかし有限非可換体は存在しえないことが証明できる (ヴェダーバーンの定理).

例　1. $p = 5$ とする. $2^2 \equiv 4, 2^3 \equiv 3 \pmod 5$ だから 2 は法 5 の原始根である. また $3^2 \equiv 4,\ 3^3 \equiv 2 \pmod 5$ だから 3 も法 5 の原始根である.

2. $p = 7$ とする. $2^2 \equiv 4, 2^3 \equiv 1 \pmod 7$ となって 2 の冪では $3, 5, 6$ の属する類は表せないから原始根ではない. $3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5$ (mod 5) となって 3 は法 7 の原始根であることがわかる.

2 は法 $3, 5, 7$ 等の原始根となるが, 無数の素数 p に対して 2 が法 p の原始根となるかどうかは未解決の問題である. $3, 5$ 等他の平方数ではない整数についても同様である.

r を法 p の原始根とするとき,

$$r^x \equiv 1 \pmod p \iff x \equiv 0 \pmod{p-1} \tag{3}$$

が成り立つことは明らかで, 後でよく使う.

定義　群 G の正規部分群 G_1, G_2 に対して，写像 $f : G_1 \times G_2 \longrightarrow G$ を $f(x_1, x_2) = x_1 x_2$ で定義する．もしもこの f が同型写像である場合には，G は部分群 G_1, G_2 の直積であると言って $G = G_1 \times G_2$ と表す．

問題　群 G とその正規部分群 G_1, G_2 に対して $G = G_1 \times G_2$ が成り立つためには次の各条件が必要十分である：

1. $x_1 x_2 = x_2 x_1$ $(\forall x_1 \in G_1, \forall x_2 \in G_2)$，かつ任意の $x \in G$ が $x = x_1 x_2$ $(x_1 \in G_1, x_2 \in G_2)$ と一意的に表せる．
2. $G_1 \cap G_2 = \{e\}$ かつ $G = G_1 G_2$ $(= G_1, G_2$ から生成される群$)$

定理 8.3　p を奇素数とするとき $(\mathbb{Z}/p^n\mathbb{Z})^\times$ は位数 $\varphi(p^n) = p^{n-1}(p-1)$ の巡回群をなす．また $(\mathbb{Z}/2^n\mathbb{Z})^\times$ は $n \leqq 2$ のとき位数 $\varphi(2^n) = 2^{n-1}$ の巡回群をなし，$n \geqq 3$ のときは位数 2^{n-2} の巡回部分群と位数 2 の巡回部分群の直積となる．

証明　p を奇素数とする．定理 8.1 によって $(\mathbb{Z}/p^n\mathbb{Z})^\times$ は位数 $p-1$ の部分群 G_1 と位数 p^{n-1} の部分群 G_2 との直積である：$(\mathbb{Z}/p^n\mathbb{Z})^\times = G_1 \times G_2$.

$f : (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ を $f(x \bmod p^n) = x \bmod p$ で定義する．この f は全射準同型であるが，その核を N とすると，核の定義から $N = \{x \bmod p^n \mid x \equiv 1 \pmod p\}$ であるから，$G_2 \subsetneqq N$ が成り立つ．($\because$ $x \in G_2 \Longrightarrow x^{p^{n-1}} \equiv 1 \pmod{p^n} \Longrightarrow x^{p^{n-1}} \equiv 1 \pmod p$. $x^p \equiv x \pmod p$ がフェルマーの小定理から成り立つから $x \equiv 1 \pmod p$. $\therefore$ $x \in N$.)

$(\mathbb{Z}/p^n\mathbb{Z})^\times/N \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ より

$$|(\mathbb{Z}/p\mathbb{Z})^\times| = ((\mathbb{Z}/p^n\mathbb{Z})^\times : N) = |(\mathbb{Z}/p^n\mathbb{Z})^\times|/|N|$$

を得る．故に $|N| = p^{n-1}$ $\therefore$ $G_2 = N$(有限集合の原理)．故に，

$$(\mathbb{Z}/p\mathbb{Z})^\times \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times/G_2 \simeq G_1 \times G_2/G_2 \simeq G_1.$$

したがって G_1 は位数 $p-1$ の巡回群である．次に

$$x^p \equiv 1 \pmod{p^n} \tag{4}$$

という合同式を考える．(4) に解 x があったとすれば $x \equiv x^p \equiv 1 \pmod p$ であるから $x = 1 + up^m, m \geqq 1, (u,p) = 1$ と書ける．

$$\begin{aligned} x^p &= 1 + p \cdot up^m + \frac{1}{2}p(p-1)(up^m)^2 + \cdot + (up^m)^p \\ &\equiv 1 + up^{m+1} \pmod{p^{m+2}} \end{aligned}$$

(4) とあわせて $m+1 \geqq n \quad \therefore \quad m \geqq n-1$．したがって (4) の解は $x \equiv 1 + jp^{n-1} \pmod{p^n}, j = 0, 1, \cdots, p-1$ と表せる．すなわちちょうど p 個の解があるから p 群 G_2 は巡回群でなければならない．以上によって G_1, G_2 はともに巡回群で位数が互いに素だから，$(\mathbb{Z}/p^n\mathbb{Z})^\times$ は巡回群である．$p=2$ の場合は読者の研究に任せよう．‖

§ 2. 平方剰余

$(\mathbb{Z}/p\mathbb{Z})^\times$ が巡回群であることの応用例として平方剰余の話をしよう．

p を奇素数とする．$a \not\equiv 0 \pmod p$ なる整数 a に対して，合同式

$$x^2 \equiv a \pmod p$$

が整数解 x を有するとき，整数 a は法 p の**平方剰余**，しからざるとき**平方非剰余**という．代数学的に言えば，体 $\mathbb{Z}/p\mathbb{Z}$ において 2 次方程式

$$x^2 = \overline{a}$$

が解を ($\mathbb{Z}/p\mathbb{Z}$ の中に) 有するとき a は平方剰余と称するのである．等式はもちろん $\mathbb{Z}/p\mathbb{Z}$ で考えている．

a が平方剰余であるか否かにしたがって

$$\left(\frac{a}{p}\right) = 1, \text{ または } -1$$

とする．この記号を，**平方剰余記号**，または**ルジャンドルの記号**という．

一般に $x^2 \equiv (p-x)^2 \pmod p$ であるから $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ が平方剰余のすべてを与える．しかもこれらは $\bmod p$ で等しくない．したがって平方剰余と非剰余とは 0 の類を数えなければちょうど同数だけある．

例　$p=5$ とする．$1^2\equiv 1, 2^2\equiv 4 \pmod 5$ だから

$$\left(\frac{1}{5}\right)=\left(\frac{4}{5}\right)=1,\ \left(\frac{2}{5}\right)=\left(\frac{3}{5}\right)=-1.$$

定義から $a\equiv b \pmod p$ ならば

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$$

であるから，$\left(\frac{*}{p}\right)$ は $(\mathbb{Z}/p\mathbb{Z})^\times$ から乗法群 $\{+1,-1\}$ の上への写像とみなせる．

定理 8.4 (**オイラーの規準**)

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$$

証明　r を法 p の原始根とし，$a\equiv r^\alpha \pmod p$ とする．

$$\begin{aligned}\left(\frac{a}{p}\right)=1 &\Longleftrightarrow \alpha\equiv 0 \pmod 2\\ &\Longleftrightarrow r^{\frac{\alpha(p-1)}{2}}\equiv 1 \pmod p \quad (\because\ r^{\frac{p-1}{2}}\equiv -1 \pmod p)\\ &\Longleftrightarrow a^{\frac{p-1}{2}}\equiv 1 \pmod p.\end{aligned}$$

$a^{\frac{p-1}{2}}\equiv \pm 1 \pmod p$ を考えれば，これで証明が終わる．‖

定理 8.5　$\left(\frac{*}{p}\right):(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ は準同型写像である．すなわち次が成り立つ：

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

証明　オイラーの規準により

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p,\quad \left(\frac{b}{p}\right)\equiv b^{\frac{p-1}{2}} \pmod p$$

$$\therefore\ \left(\frac{ab}{p}\right)\equiv (ab)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}\cdot b^{\frac{p-1}{2}}\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

$$\therefore\ \left(\frac{ab}{p}\right)\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

平方剰余記号の値は ± 1 だから定理が成り立つ．‖

次の定理はガウスによって証明されたもので，(代数的整数論以前という意味で) 古典的整数論の頂点を示すものである．

定理 8.6 (平方剰余の相互法則)　p, q を奇素数とすると

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

定理 8.7 (補充法則)　p を奇素数とすると

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \text{(第 1 補充法則)}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \text{(第 2 補充法則)}$$

第 1 補充法則はオイラー規準から明らか．

この 2 定理によって平方剰余記号は簡単に計算される．整数 a が p を法として平方剰余であるかどうかを判定するというだけの見地なら，$\bmod p$ で考えれば簡単にすべての場合を尽せるわけだから，相互法則が「黄金律」(ガウス) とまで呼ばれる理由はない．ガウスは円分体の相互法則まで見通していたとまでは思わないが，当時の知識を超えた「何か」を感じ取っていたに違いない．そしてまた一方では，円分体の相互法則，さらには類体論の相互法則がガウスが予見した理想郷の実現であるという保証もない．証明は初等的なものもガウス以来いくつか知られているが本質的だとは言えないように思う．つまり $\left(\frac{q}{p}\right)$ は p を法としての話なのに，なぜ q を法として決まる値 $\left(\frac{p}{q}\right)$ で計算されてしまうのか，証明を読んでも腑に落ちない，「どうしてそうなるの ?」とキツネに化かされたような心地が後味として残るという意味である．これは初等数論的技巧の通弊である．定理をより深く理解するためには証明を知ることだとはよく言われるが，それには腑に落ちる証明であることが必要であろう．後に円分体論による証明を紹介しよう．初等的とは言えないが，証明の意味が納得できるという意味において本書の目論見にピッタリの題材である．

第9章　アーベル群の基本定理の証明

§ 1. 有限生成アーベル群の基本定理の証明 (前半)

定義　加群 M はある自然数 r に対して $M \simeq \mathbb{Z}^r$ が成り立つとき階数 r の**自由加群** (演算が $+$ で書かれているとは限らぬ場合は**自由アーベル群**) と呼ばれる．単位元だけからなる群は階数 0 の自由加群としておく．

次の定理は基本定理の証明の一部だが，それ自身重要である．

定理 9.1　階数 r の自由加群の部分群は階数 s $(s \leqq r)$ の自由加群である．

証明　M を階数 r の自由加群とし，$\{m_1, \cdots, m_r\}$ をその一組の基底とする．すなわち，M の任意の元は $x_1m_1 + \cdots + x_rm_r$ の形にただ一通りの方法で表されるとする．これは M が $\mathbb{Z}^r = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (r 個の直和) と同型だから可能で，$(0, \cdots, 1, \cdots, 0)$ (i 番目だけ 1) に対応する M の元を m_i とすればよいのである．

N を M の部分加群とする．N の元であって $xm_1 (x \in \mathbb{Z})$ という形に書ける元の全体を N_1 とする：

$$N_1 = \{y(\in N) \mid \exists x(\in \mathbb{Z}); y = xm_1\} = N \cap \mathbb{Z}m_1$$

単射 $p_1 : N_1 \longrightarrow \mathbb{Z}$ を $xm_1 \rightsquigarrow x$ によって定義する．$p_1(N_1)$ は簡単にわかるように $\mathbb{Z}$ のイデアルをなすから $p_1(N_1) = (a_1)$ なる $a_1 \in \mathbb{Z}$ が取れる．

$n_1 \in N_1$ を $p_1(n_1) = a_1$ を満たす元とする．すると $N_1 = \mathbb{Z}n_1 = \{xn_1 \mid x \in \mathbb{Z}\}$ である．

この操作を延長して次のようにしよう．

$$N_i = N \cap (\mathbb{Z}m_1 + \cdots + \mathbb{Z}m_i) \quad (i = 2, 3, \cdots, r)$$

と置く．つまり $(x_1m_1 + \cdots + x_im_i$ という形に書ける N の元の全体を N_i とする．$y = x_1m_1 + \cdots + x_im_i \in N_i$ に対して x_i を対応させる写像を $p_i : N_i \longrightarrow \mathbb{Z}$ と記す．p_i は準同型写像で像 $p_i(N_i)$ は $\mathbb{Z}$ のイデアルをなす．したがって $p_i(N_i) = (a_i)$ と表せる．$n_i \in N_i$ を $p_i(n_i) = a_i$ なる元とする．ただし，もしも $a_i = 0$ であれば $n_i = 0$ とする．すると

$$N_i = N_{i-1} \oplus \mathbb{Z}n_i$$

である．すなわち

$$N_{i-1} \cap \mathbb{Z}n_i = \{0\}$$

かつ

$$N_i = N_{i-1} + \mathbb{Z}n_i = \{x + zn_i \mid x \in N_{i-1}, z \in \mathbb{Z}\}$$

である．(p.118 の問題参照.) このとき，

$$\begin{aligned} N = N_r = N_{r-1} \oplus \mathbb{Z}n_r &= N_{r-2} \oplus \mathbb{Z}n_{r-1} \oplus \mathbb{Z}n_r = \cdots \\ &= \mathbb{Z}n_1 \oplus \cdots \oplus \mathbb{Z}n_r \end{aligned}$$

$n_i = 0$ ならば, もちろん $\mathbb{Z}n_i = \{0\}$．そこで $n_i \neq 0$ とする．このとき $\mathbb{Z}n_i \simeq \mathbb{Z}$ が成り立つ．以上によって 0 でない n_i の数を s とすれば $s \leqq r$ で $N \simeq \mathbb{Z}^s$ が言えた． ‖

定理 9.2　M を階数 r の自由加群，N を M の部分加群とし，その階数は同じく r であるとする．M の $\mathbb{Z}$ 上の基底を $\{m_1, \cdots, m_r\}$ とし，

$$\left\{ \sum_{j=1}^{r} a_{1j}m_j, \cdots, \sum_{j=1}^{r} a_{rj}m_j \right\} \quad (a_{ij} \in \mathbb{Z})$$

が N の基底をなすものとすれば

$$(M : N) = |\det(a_{ij})|$$

が成り立つ．ここに $\det(a_{ij})$ は r 次正方行列 (a_{ij}) の行列式，また $(M : N)$ は商群 M/N の位数，すなわち N による剰余類の個数である．

証明　定理9.1の証明によれば N の基底として

$$\begin{cases} n_1 = a_1 m_1 \\ n_2 = a_{21} m_1 + a_2 m_2 \\ \quad\vdots \\ n_r = a_{r1} m_1 + \cdots + a_r m_r \end{cases}$$

という形のものが取れる．ただし，$a_j > 0$ とする．しからば M/N の代表系として

$$\{b_1 m_1 + \cdots + b_r m_r \mid 0 \leqq b_j < a_j \ (j = 1, \cdots, r)\}$$

が取れることがわかる．なぜなら $x = c_1 m_1 + \cdots + c_r m_r$ を M の任意の元として，

$$c_r = q_r a_r + b_r, \quad 0 \leqq b_r < a_r$$

と表すと，

$$x - q_r n_r = c_1^{(1)} m_1 + \cdots + c_{r-1}^{(1)} m_{r-1} + b_r m_r$$

すなわち，

$$x \equiv c_1^{(1)} m_1 + \cdots + c_{r-1}^{(1)} m_{r-1} + b_r m_r \pmod N$$

となる．($x \equiv y \pmod N$ は $x - y \in N$ の意である．)

$$c_{r-1}^{(1)} = q_{r-1} a_{r-1} + b_{r-1}, \quad 0 \leqq b_{r-1} < a_{r-1}$$

とすれば同様に

$$x \equiv c_1^{(2)} m_1 + \cdots + c_{r-2}^{(2)} m_{r-2} + b_{r-1} m_{r-1} + b_r m_r \pmod N$$

となる．これを続ければ

$$x \equiv b_1 m_1 + \cdots + b_r m_r \pmod N$$

しかも $0 \leqq b_j < a_j \ (j = 1, \cdots, r)$ となる．そしてこれらは同じ N を法として類に落ちることはないので代表の個数は $a_1 \cdots a_r$ でしかも

$$\begin{vmatrix} a_1 & 0 & \cdots & 0 \\ a_{21} & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_r \end{vmatrix} = a_1 a_2 \cdots a_r$$

である．次の問題を参考にすれば証明は終わる．‖

問題　$\left\{\sum_{j=1}^{r} a_{1j}m_j, \cdots, \sum_{j=1}^{r} a_{rj}m_j\right\}, \left\{\sum_{j=1}^{r} b_{1j}m_j, \cdots, \sum_{j=1}^{r} b_{rj}m_j\right\}$ がともに N の基底をなせば

$$|\det(a_{ij})| = |\det(b_{ij})|$$

［ヒント］　第一の基底を $\{n_1, \cdots, n_r\}$，第二の基底を $\{n'_1, \cdots, n'_r\}$ とし，$A = (a_{ij}), B = (b_{ij})$ と置くと

$$\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = A \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}, \quad \begin{pmatrix} n'_1 \\ \vdots \\ n'_r \end{pmatrix} = B \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

しかも

$$\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = P \begin{pmatrix} n'_1 \\ \vdots \\ n'_r \end{pmatrix}, \quad \begin{pmatrix} n'_1 \\ \vdots \\ n'_r \end{pmatrix} = Q \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$$

と表せる．ここに P, Q は成分が整数で $|P| = \pm 1$, $|Q| = \pm 1$.

§2. 森さんのことなど

本書の元になった連載中，普段より良く『数セミ』を読むようになった．中でも草場公邦さん，森毅さん，倉田令二郎さんの三人の書く文章には感心させられた．

倉田，というのはもちろんあの，「ついに悪の華咲くバビロンのカーニバルと縁を切り——少なくともそのようなふりをして——九州は博多へと流れて行くところで私の前半生は終る．云々」(『数学セミナー』，'78 年 9 月号)，という格調高い名文を書いた倉田令二朗である．あの記事は何やら訳がわからんという声を二，三聞いたが私にはわかりやすかった．

倉田さんがケバケバしいが隙がなく鍛錬された文章を書く代表とすれば，

かたや草場公邦氏はフラフラ，隙だらけ，天衣無縫，正直の代表である．彼は最近『数理と発想』(創拓社刊) という随筆集を出版した．大したことは書いてないが本人の人柄がにじみ出た文章で好感が持てる．

「身体が少々長いせいか，家の中ではたいてい長椅子に寝転がって煙草を吸っている．鯨が潮を吹いているのと似たようなものである．(中略) これはぼくの飛躍を待つ憧憬の完成された一つの型式なのである．」

そこで奥さんに無理やり「バーへでも行ってこい」と押し出されて家を出るがそう大しておもしろいこともなく，といった調子．私のように英語 3 時間，ランニング 1 時間，碁 2 時間，あるときは書，ある時はオルガンとたゆみなく努力のための努力を続ける人間と何とまあ異質の世界なのであろうか．草場さんは奥さんが息子に毎日ピアノの練習をさせるのを「いじましい」とかなんとか，そんな言葉を吐いてひどくいやがっていた．努力するというのがえらくいやなのだそうだ．私も彼からみれば「いじましい」人間なのであるが，一言自己弁護するなら，たとえば，もちろん英語が人よりできるようになりたいが，むしろ大部分はただ熱中すること自体がおもしろいというだけのことなのだ．(もちろん何の上達も感じられなければ話にならない)

草場さんの随筆には天才とか秀才とかについての考察にかなりのペースが割かれている．私もそりゃ秀才でありたいけれども目標を立てて「一人で」毎日寸暇を惜んで努力する，その努力すること自身が楽しいのである．他人ないし自分が秀才であろうが天才であろうが 40 歳にもなって何をいまさらという気がする．

なぜそんなに努力したいのだろうか，と自らに問うてみる．どうも基本的には私は極端な厭世家，厭人屋らしいのだ．人とつきあうのが下手で，そのくせおしゃべりなので人といるとどうして良いかわからんのでおしゃべりをし，それを武器としてバリヤを張っているのである．人も私といると疲れるだろうが，私の方も家にいるとほっとするのである．そして自分を相手に限りなく競争し，以前より何かしら新しく知ったり進歩したりするのが無性にうれしいらしい．

草場さんの話から随分ずれてしまった．彼の本は数学者の書いた随筆の中では白眉である．彼はのほほんとした純粋培養人間という意味で数学者の典型である．社会的には音痴でしかも無知だという意味でも典型である．そういう数学者の長所・短所を丸出しにしているところが彼の美点であり，この本の特徴なのである．とにかく，この本がベストセラーになるとは思えないのでみなさん数学愛好家のよしみで買ってやってください．

京都の森，と言えばもちろん誰もが知っている通り，一刀斎とも森毅とも呼ばれる二つ名前のあの森さんである．

> それでも試験を受けてそのままで，卒業の前に単位が取れるかどうか彌永 (昌吉) さんのところに聞きにいくと，ア，えーと，モ，森君と言いましたっけ，たしかあの答案は，とそこらに散らばった紙クズを探しまわったところで，出てくる道理もない．そのエート，できましたか，なんて聞かれて，こっちも，2 年前のことでよう覚えてませんが，易しい問題は忘れましたけど，一題はたしかこんな問題で，はじめこんなにしてやりかけて失敗したので，方針を変えてこないにしたらまあなんとか，といった説明をすると，さすが心やさしき彌永先生，あ，それなら優にしときます，もっとも何もせんでも優だという説もあった．古きよき時代よ．(『数学セミナー』，’77 年 7 月号)

といった調子．思わず吹き出した．雰囲気がよく出ている．彌永先生に聞いたら覚えがないといっておられた．しかし森さんがデッチアゲたのだとすると，いくらなんでも文章がさえ過ぎている．どうも彌永先生あちこちでそういう恩恵をほどこしすぎて忘れてしまわれたというのが真相ではあるまいか．

前のことを思い出して森さんの文章を引用しようと雑誌をひっくり返したついでに幾人かの文章を読んでいたら，うまい文章だと思われるのはその人の語り口をほうふつとさせるときだということに気がついた．だから書いた人なり書かれた人なりを知っていなければそれほど面白くも可笑しくもないかもしれない．その正否はその人を現に知っているのだから，いまさら確か

めようもない．

森さんの本でちゃんと読んだのは『異説 数学者列伝』(蒼樹書房) だけであるが，そのまえがきがやっぱりよかった．

「だいたい，科学者の伝記では，エライ人だけれどもヘンなところもある，というパターンが多い．ぼくはこれは気に入らない．まあ少しはヘンなところもある普通のありふれた人間，つまり，よくあるヘンな奴だけども，エライところもある，という方がよいと思う．」

まったくその通りだ．碁・将棋のような芸事にしたってそうで，大体下手な講談師が破れた扇子をたたく調子の神技・鬼手・奇伝の扇動が過ぎる．

森さんのこの本は「エジプト 12 面体の秘密」(これはクィーンのモジリ)，「旅占星師に初雪が舞った」(これは木枯紋次郎であろう) と各数学者に奇妙なモジリ題名を冠した 30 編からなる愉快な本だ．かなり創作，すなわちデッチアゲも含まれていそうな匂いがするが，そういうインチキくさい (しかし実際は裏打ちがしっかりした) ところが森さんの持ち味である．一体に森さんは目の付けどころがいい．心の機微にふれた題材が多い．ただ，「日本三ワカラン」の一人ともう一つ異名をとっているように，意味不明な個所が特に数学のこととなると多いので読む人は気にしないことが大切．

森さんは酒が飲めない．酒で泣きの入っていない人間にはロクな奴はいないというのが私の持論だが，森さんはその説の当てはまらない珍しい例外である．飲みもしないでどうしてあんなにヨッパラッていられるのか，不思議なことがあるものである．ただ，心の機微にふれた題材が多い，目の付けどころがいいと書いたのだが，もしも森さんが酒飲みであったなら中味にもっと陰翳が…，と惜しまれる．

§ 3. アーベル群の基本定理の証明 (後半)

M を有限生成の加群とし，$m_1, \cdots, m_n$ をその生成系としよう：

$$M = \mathbb{Z}m_1 + \cdots + \mathbb{Z}m_n$$

$f : \mathbb{Z}^n \longrightarrow M$ を $f(x_1, \cdots, x_n) = x_1 m_1 + \cdots + x_n m_n$ で定義する．f は上への準同型写像である．f の核 $\ker f$ は自由加群 $\mathbb{Z}^n$ の部分加群だから定理 9.1 によって階数 m ($\leqq n$) の自由加群である．そこで仮りに $\mathbb{Z}^n$ の基底 $\{\overrightarrow{a}_1, \cdots, \overrightarrow{a}_n\}$ と自然数 $d_1, \cdots, d_m$(ただし $d_j | d_{j+1}, j = 1, \cdots, m-1$) とを上手に選んで $\{d_1 \overrightarrow{a}_1, \cdots, d_m \overrightarrow{a}_m\}$ が $\ker f$ の基底になるようにできるならば話は簡単である：

$$\begin{aligned} M &\simeq \mathbb{Z}^n / \ker f \\ &= (\mathbb{Z}\overrightarrow{a}_1 \oplus \cdots \oplus \mathbb{Z}\overrightarrow{a}_n)/(\mathbb{Z}d_1\overrightarrow{a}_1 \oplus \cdots \oplus \mathbb{Z}d_m\overrightarrow{a}_m) \\ &\simeq \mathbb{Z}\overrightarrow{a}_1/\mathbb{Z}d_1\overrightarrow{a}_1 \oplus \cdots \oplus \mathbb{Z}\overrightarrow{a}_m/\mathbb{Z}\overrightarrow{a}_m \oplus \mathbb{Z}^r \quad (r = n - m) \\ &\simeq \mathbb{Z}/\mathbb{Z}d_1 \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}d_m \oplus \mathbb{Z}^r \end{aligned}$$

以上において準同型定理，および

$$G_1 \oplus \cdots \oplus G_n / N_1 \oplus \cdots \oplus N_n \simeq G_1/N_1 \oplus \cdots \oplus G_n/N_n,$$

$\mathbb{Z}/(0) \simeq \mathbb{Z}$ などを用いた．$\mathbb{Z}\overrightarrow{a}/\mathbb{Z}d\overrightarrow{a} \simeq \mathbb{Z}/\mathbb{Z}d$ も準同型定理によって証明される．

$d_i = 1$ ならば $\mathbb{Z}/\mathbb{Z}d_i \simeq \{0\}$ なので，これは取り除くことができるから $d_1 > 1$ としてよい．このとき $d_j | d_{j+1}$ と仮定したので，アーベル群の基本定理が分解の一意性を除けば証明されたことになる．

$$M \simeq \mathbb{Z}/\mathbb{Z}d'_1 \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}d'_{m'} \oplus \mathbb{Z}^{r'}$$

をもう一つの分解とする．$d_m \cdot \mathbb{Z}/d_i\mathbb{Z} = \{0\}$ だから，

$$d_m M \simeq d_m \mathbb{Z}^r \simeq \mathbb{Z}^r$$

同様にして $d'_{m'} M \simeq \mathbb{Z}^{r'}$.

$$\therefore\ d_m d'_{m'} M \simeq \mathbb{Z}^r,\ d_m d'_{m'} M \simeq \mathbb{Z}^{r'}$$

$$\therefore \quad \mathbb{Z}^r \simeq \mathbb{Z}^{r'}. \quad \therefore \quad r = r'.$$

(最後の $r = r'$ を導くに際して，ベクトル空間の次元の一意性を使った.) 任意の $k \in \mathbb{N}$ に対する $k\overrightarrow{x} = \overrightarrow{0}$ の解の個数を調べて $m = m', d'_j = d_j$ を得る．

以上を振り返れば，つぎの定理が示されればよいことになった：

定理 9.3　M を階数 r の自由加群，N を M の階数 s の部分加群とすると M の基底 $\{m_1, \cdots, m_r\}$ と自然数 $d_1, \cdots, d_s$ $(d_j | d_{j+1};\ j = 1, 2, \cdots, s-1)$ を $\{d_1 m_1, \cdots, d_s m_s\}$ が N の基底をなすように選ぶことができる．

まず M, N の基底を任意にとって $\{m_1, \cdots, m_r\}, \{n_1, \cdots, n_s\}$ とする．各 $n_j \in M$ だから

$$\begin{pmatrix} n_1 \\ \vdots \\ n_s \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{s1} & \cdots & a_{sr} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}, \quad a_{ij} \in \mathbb{Z}\ (i = 1, \cdots, s; j = 1, \cdots, r)$$

と表すことができる．

$A = (a_{ij})$ と置く．$SL_\ell(\mathbb{Z})^\pm$ によって，整数を成分にもち，しかも行列式が ± 1 の ℓ 次正方行列の全体のなす群を表すことにする．

いま $P \in SL_s(\mathbb{Z})^\pm$ を任意に取る．すると

$$\begin{pmatrix} n'_1 \\ \vdots \\ n'_s \end{pmatrix} = P \begin{pmatrix} n_1 \\ \vdots \\ n_s \end{pmatrix} = PA \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

によって定まる $\{n'_1, \cdots, n'_s\}$ も N の基底をなす．また $Q \in SL_r(\mathbb{Z})^\pm$ を任意に取る．すると

$$\begin{pmatrix} m'_1 \\ \vdots \\ m'_r \end{pmatrix} = Q^{-1} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix},\ \text{したがって}\ \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = Q \begin{pmatrix} m'_1 \\ \vdots \\ m'_r \end{pmatrix}$$

によって決まる $\{m'_1, \cdots, m'_r\}$ も M の基底をなす．このとき，

$$\begin{pmatrix} n'_1 \\ \vdots \\ n'_s \end{pmatrix} = PAQ \begin{pmatrix} m'_1 \\ \vdots \\ m'_r \end{pmatrix}$$

であるから，定理 9.3 は次の行列の問題に還元される：

定理 9.4　整数を成分に持つ $m \times n$ 行列 A に対し

$$PAQ = \left(\begin{array}{ccc|c} d_1 & \cdots & 0 & \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & d_r & \\ \hline & 0 & & 0 \end{array}\right), \ d_j | d_{j+1} \quad (j = 1, \cdots, r-1)$$

を満たす整数成分の m 次行列 P, n 次行列 Q (ただし $|P| = \pm 1$, $|Q| = \pm 1$) が存在する.

証明　A に行基本変形 (二つの行を入れ換える. 一つの行の整数倍を他の行に加える, ある一つの行を -1 倍する) を行うことは, ある P ($|P| = \pm 1$) を左から A に掛けることを意味する. A に列基本変形を行うことはある Q ($|Q| = \pm 1$) を右から A に掛けることを意味する.

そこで A の成分 a_{ij} の中で $|a_{ij}|$ が最小正のものを取り, それを $(1,1)$ 成分に持っていく. それを改めて a_{11} とする. 第 1 列, 第 1 行の中に a_{11} の倍数ではないものがあれば, それをたとえば a_{1k} とする. 割算の原理を用いて

$$a_{1k} = qa_{11} + r, \quad 0 < r < |a_{11}|$$

と表す. A の第 1 列の q 倍を第 k 列から引けば $(1,k)$ 成分は r となる. そこでこれを $(1,1)$ へ持っていって a_{11} とする. この操作を繰り返せばもとの $|a_{11}|$ より小さい自然数は有限個なので, そのうち第 1 列, 第 1 行はすべて a_{11} の倍数となる. したがって第 1 列, 第 1 行はすべて $(1,1)$ 成分以外は 0 としてよいことになる.

これまでの操作を何度か繰り返すことによって第 1 列, 第 1 行は $(1,1)$ 成分以外は 0 で, 第 2 行以下, 第 2 列以下の成分はすべて a_{11} の倍数となるようにできる.

あとは第 2 行以下と第 2 列以下にこの操作を行って結局 A は定理の形にまで持って行けることがわかる. ∥

§ 4. 整数基について

自由加群の例として代数体の整数環を取り上げよう.

代数体 K の共役写像を $(1), \cdots, (n)$ で表す. ここに $n = [K:\mathbb{Q}]$ とする.

定義　$\alpha_1, \cdots, \alpha_n (\in K)$ に対して

$$d(\alpha_1, \cdots, \alpha_n) = \begin{vmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_n^{(1)} \\ & \cdots\cdots\cdots & & \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \cdots & \alpha_n^{(n)} \end{vmatrix}^2 = (\det(\alpha_j^{(i)}))^2$$

と定義し, $\alpha_1, \cdots, \alpha_n$ の**判別式**と呼ぶ.

命題　$d(\alpha_1, \cdots, \alpha_n)$ は有理数である.

証明 (ガロアの理論を使う)　$K \subsetneqq L$ なるガロア拡大 $L/\mathbb{Q}$ を取る. $L/\mathbb{Q}$ のガロア群 $G(L/\mathbb{Q})$ の元 σ を判別式 $d(\alpha_1, \cdots, \alpha_n)$ にほどこすと行が入れ換わるが, 判別式は, 行列式を平方しているので, 値が不変である. 任意の $\sigma \in G(L/\mathbb{Q})$ に対して値が不変なのだから, ガロアの理論によって $d(\alpha_1, \cdots, \alpha_n) \in \mathbb{Q}$ である. ‖

定理 9.5　n 次の代数体の整数環は階数 n の自由加群をなす.

$[K:\mathbb{Q}] = n$ のとき代数体 K は $\mathbb{Q}$ 上 n 次であるという. K の代数的整数の全体は環をなす. これを K の整数環といって $\mathbb{O}_K$ と表すのであった.

証明の前につぎの問題を考えよ.

問題　次を示せ：

$$\exists\alpha_1 \cdots \exists\alpha_n (\in \mathbb{O}_K);\ d(\alpha_1, \cdots, \alpha_n) \neq 0$$

[ヒント]　$K = \mathbb{Q}(\omega)$ とする. $\omega \in \mathbb{O}_K$ としてよい. (p.102 の問題参照.) $d(1, \omega, \omega^2, \cdots, \omega^{n-1})$ はヴァンデルモンド型の行列式の平方であるから, そ

の値は $\left(\prod_{j>i}(\omega^{(j)}-\omega^{(i)})\right)^2$ であって，これは 0 でない．

問題　$\alpha_1,\cdots,\alpha_n(\in K)$ が K の $\mathbb{Q}$ 上の基底をなすためには

$$d(\alpha_1,\cdots,\alpha_n)\neq 0$$

が必要十分である．

［ヒント］　$K=\mathbb{Q}(\theta)$ とする．

$$\alpha_j=\sum_{i=0}^{n-1}a_{ij}\theta^i\ (j=0,1,\cdots,n-1)$$

なる $a_{ij}\in\mathbb{Q}$ が取れることから

$$d(\alpha_1,\cdots,\alpha_n)=(\det(a_{ij}))^2 d(1,\theta,\cdots,\theta^{n-1}).$$

証明 (定理 9.5 の証明)　$\alpha_1,\cdots,\alpha_n$ が代数的整数ならそれらの共役数も代数的整数で，したがって $d(\alpha_1,\cdots,\alpha_n)$ は代数的整数かつ有理数，すなわち有理整数である．$|d(\alpha_1,\cdots,\alpha_n)|\neq 0$ が最小正となるような $\alpha_1,\cdots,\alpha_n$ ($\in\mathbb{O}_K$) の組を一組取る．このとき $\alpha\in\mathbb{O}_K$ はすべて

$$\alpha=a_1\alpha_1+\cdots+a_n\alpha_n,\ a_1,\cdots,a_n\in\mathbb{Z} \tag{1}$$

という形に表されることを証明したい．

まず上の問題によって $\alpha_1,\cdots,\alpha_n$ が K の $\mathbb{Q}$ 上の基底であることはわかっている．$\alpha\in\mathbb{O}_K$ を $\alpha=a_1\alpha_1+\cdots+a_n\alpha_n$ と表したときに $a_1,\cdots,a_n$ の中に整数でないものがあったとして，たとえば $a_1\notin\mathbb{Z}$ とする．

$$a_1=a+r,\ a\in\mathbb{Z},\ 0<r<1$$

と書いてみる．$\alpha-a\alpha_1(=r\alpha_1+\cdots)\in\mathbb{O}_K$ で

$$\begin{aligned}|d(\alpha-a\alpha_1,\alpha_2,\cdots,\alpha_n)|&=|d(r\alpha_1+\cdots,\alpha_2,\cdots,\alpha_n)|\\&=|d(\alpha_1,\alpha_2,\cdots,\alpha_n)|\cdot r^2<|d(\alpha_1,\alpha_2,\cdots,\alpha_n)|\end{aligned}$$

これは $\alpha_1,\cdots,\alpha_n$ の選び方に矛盾する．故に $\mathbb{O}_K$ のすべての元が (1) の形に表せることがわかった．表し方の一意性は $[K:\mathbb{Q}]=n$ から明らか．‖

$\mathbb{O}_K$ の自由加群としての基底，すなわち $\mathbb{O}_K$ の元をすべて (1) の形に一意的に表せる $\alpha_1, \cdots, \alpha_n$ の組を**整数基**という．

$\{\alpha_1, \cdots, \alpha_n\}, \{\beta_1, \cdots, \beta_n\}$ を二組の整数基とする．すると

$$\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i, \quad \alpha_j = \sum_{i=1}^{n} b_{ij}\beta_i \quad (j = 1, 2, \cdots, n)$$

ここに $a_{ij} \in \mathbb{Z}, b_{ij} \in \mathbb{Z}$ と表せる．これによって

$$\det(a_{ij})\det(b_{ij}) = 1 \quad \therefore \quad \det(a_{ij}) = \pm 1$$

がわかる．したがって

$$d(\alpha_1, \cdots, \alpha_n) = d(\beta_1, \cdots, \beta_n)$$

を得る．すなわち $d(\alpha_1, \cdots, \alpha_n)$ は K の整数基の選び方には依存しない．この値を代数体 K の**判別式**と言い，D_K と表す．

例題　$K = \mathbb{Q}(i)$ の整数基と判別式を求めよ．

解答　$\alpha = a + bi \ (a, b \in \mathbb{Q})$ に対して $\alpha' = a - bi$ とする．

$$\begin{aligned} \alpha \in \mathbb{O}_K &\iff \alpha + \alpha' \in \mathbb{Z}, \quad \alpha\alpha' \in \mathbb{Z} \\ &\iff 2\alpha \in \mathbb{Z}, \quad a^2 + b^2 \in \mathbb{Z} \end{aligned}$$

このとき

$$(2a)^2 + (2b)^2 \in \mathbb{Z} \quad \therefore \ (2b)^2 \in \mathbb{Z} \quad \therefore \ 2b \in \mathbb{Z}$$

そこで $a = c/2, b = d/2$ と置くと，$a^2 + b^2 \in \mathbb{Z}$ より

$$c^2 + d^2 \equiv 0 \pmod 4$$

$$\therefore \quad c \equiv 0 \pmod 2, \ d \equiv 0 \pmod 2$$

$$\therefore \quad a \in \mathbb{Z}, \ b \in \mathbb{Z}$$

以上で $\mathbb{O}_K = \mathbb{Z}[i]$ がわかった．故に $\{1, i\}$ は $\mathbb{Q}(i)$ の整数基，そして判別式 D_K は

$$D_K = d(1, i) = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = -4$$

問題　$\mathbb{Q}(\sqrt{5})$ の整数基と判別式を求めよ．

答は $\{1, (1+\sqrt{5})/2\}$ がその一つである．判別式は 5．これらの計算を一般的に行うと次を得る．

定理 9.6　m は平方因子を含まない整数とし，$K = \mathbb{Q}(\sqrt{m})$ と置く．このとき

$$m \not\equiv 1 \pmod 4 \text{ ならば } \mathbb{O}_K = \{x + y\sqrt{m} \mid x \in \mathbb{Z}, y \in \mathbb{Z}\}$$
$$m \equiv 1 \pmod 4 \text{ ならば } \mathbb{O}_K = \left\{\frac{x + y\sqrt{m}}{2} \mid x, y \in \mathbb{Z}, x \equiv y \pmod 2\right\}$$

したがって $m \not\equiv 1 \pmod 4$ ならば $\{1, m\}$ を，$m \equiv 1 \pmod 4$ ならば $\left\{1, \dfrac{1+\sqrt{m}}{2}\right\}$ を K の整数基として取ることができる．

判別式はそれぞれ $4m, m$ となる．

証明は自分で挑戦されるのが一番望ましい．とにかく読者の勉強に任せよう．2 次体というのはこのように他の代数体と較べるとあらゆる点で取り扱いが易しいので，その分早くから深い結果が知られているのである．

§ 5. 単数群の構造

K を代数体とし，U_K を K の単数のなす乗法群 (**単数群**) とする：

$$U_K = \{\alpha \in \mathbb{O}_K \mid \alpha^{-1} \in \mathbb{O}_K\}$$

K の共役体のうち実数体 $\mathbb{R}$ に含まれるものが s 個，含まれないものが $2t$ 個，合計 $s + 2t = n$ とする．$a + bi$ が有理係数多項式の解ならば $a - bi$ も解だったから実数体の部分体でないものは必ず偶数個なのである．そこで

$$r = s + t - 1$$

と置く．つぎの定理は基本的である．

定理 9.7 (ディリクレの単数定理)　K を n 次代数体とすると，単数群 U_K は K に含まれる 1 の冪根のなす部分群 W_K と階数 r の自由アーベル群をなす部分群との直積である．

階数 r の自由アーベル群の基底となる単数系 $\{u_1, \cdots, u_r\}$ を K の**基本単数系**と呼ぶ.

問題　W_K は有限巡回群であることを示せ.

[ヒント]　定理 8.2.

2次体 $K = \mathbb{Q}(\sqrt{m}), m \in \mathbb{Z}$ において $m < 0$ ならば $s = 0, t = 0$ だから, $r = 0$ となり, $U_K = W_K$. しかも1の冪根であって2次方程式を満たすものは $\pm i, (\pm 1 \pm \sqrt{3}i)/2$, したがって $\mathbb{Q}(i), \mathbb{Q}(\sqrt{3}i)$ 以外の虚2次体 K では $U_K = \{\pm 1\}$ となる. $m > 0$ の場合は $r = 1$ となり, U_K は無限群ということになる. これが実2次体をして虚2次体より研究困難ならしめるほとんどただ一つの, しかも大きな障碍物なのである.

例　$K = \mathbb{Q}(\sqrt{2})$ とする. $\varepsilon = 1 + \sqrt{2}$ と置けば

$$\varepsilon\varepsilon' = (1 + \sqrt{2}) \cdot (1 - \sqrt{2}) = -1, \quad \therefore \quad \varepsilon \in U_K \text{ かつ } \varepsilon > 1$$

いま $\eta \in U_K$ とする. $|\eta| < 1$ ならば $\pm\eta^{-1}$ を考えて1より大にできる. そこで $\eta > 1$ とする. $\eta = x + y\sqrt{2}$ $(x, y \in \mathbb{Z})$ かつ $\eta \leqq \varepsilon$ とすれば $|\eta'| < 1$ より

$$-1 < x - y\sqrt{2} < 1, \ \ 1 < x + y\sqrt{2} \leqq 1 + \sqrt{2}$$

したがって

$$0 < x < (2 + \sqrt{2})/2, \ \ 0 < y < (2 + \sqrt{2})/2$$

$$\therefore \quad x = y = 1 \quad \therefore \quad \eta = \varepsilon$$

これによって $\varepsilon = 1 + \sqrt{2}$ が $\mathbb{Q}(\sqrt{2})$ の基本単数なることを知る.

さて定理の証明に戻ろう. U_K は乗法群で扱いにくい. そこで K の共役写像を

$$(1), \cdots, (s), \ (s+1), \ (s+t+1), \cdots, \ (s+t), \ (s+2t)$$

と並べる．ただし $(s+j)$ と $(s+t+j)$ とは複素共役で対の関係 $(a+bi \longleftrightarrow a-bi)$ にあるとする．$u \in U_K$ に $\mathbb{R}^{r+1}$ の元

$$(\log|u^{(1)}|,\ \cdots,\ \log|u^{(s)}|,\ \log|u^{(s+1)}|^2,\ \cdots,\ \log|u^{(s+t)}|^2)$$

を対応させる写像 $\Phi: U_K \longrightarrow \mathbb{R}^{r+1}$ を考える．明らかに

$$\Phi(uv) = \Phi(u) + \Phi(v)$$

が成り立つから Φ は乗法群 U_K から加群 $\mathbb{R}^{r+1}$ への準同型写像である．ところが Φ の核 $\{u \in U_K \mid \Phi(u) = \overrightarrow{0}\}$ は W_K であることが証明される(その証明は後に述べる)．すなわちすべての共役数が単位円周上にある代数的整数は 1 の冪根だけである．

そして $u \in U_K$ のとき

$$\begin{aligned}\log|u^{(1)}| + \cdots + \log|u^{(s)}| + \log|u^{(s+1)}|^2 + \cdots + \log|u^{(s+t)}|^2 \\ = \log|\prod_{j=1}^{n} u^{(j)}| \quad (\because\ |u^{(s+j)}| = |u^{s+t+j}|) \\ = \log 1 = 0\end{aligned}$$

である．これは $u \in U_K$ ならば $u^{-1} \in \mathbb{O}_K$ より単数 u を定める整係数モニック原始多項式の定数項は ± 1 であることからわかることである．だから Φ による U_K の像 $\Phi(U_K)$ は

$$\mathbb{H} = \{(x_1, \cdots, x_{r+1}) \in \mathbb{R}^{r+1} \mid x_1 + \cdots + x_{r+1} = 0\}$$

の部分加群である．$\mathbb{H}$ は $\mathbb{R}$ 上 r 次元のベクトル空間であるが，実は $\Phi(U_K)$ は階数 r の自由加群をなすことが証明される．

故に，群の準同型定理によって，$U_K/W_K \simeq \Phi(U_K)$ は階数 r の自由アーベル群である．U_K/W_K の基底を

$$\overline{u_i} = u_i W_K \quad (i = 1, \cdots, r)$$

とする．そして $u_1, \cdots, u_r$ から生成される群を H_K とすれば，H_K は $u_1, \cdots, u_r$ を基底とする自由アーベル群をなし，$H_K W_K = U_K$ が成り立つ．一方 W_K は有限群なので $H_K \cap W_K = \{1\}$ である．これによって $U_K = H_K \times W_K$ が得られて，定理の証明が完結する．これが証明の道筋である．しかし，$\Phi(U_K)$ が階数 r の自由加群をなすことを一般の場合に証明するのはやっか

いなので専門書に任せることにして, 実2次体の場合に限ってやってみよう. これでも雰囲気は十分に伝わるだろう.

次の補題は一般の代数体でも簡単に示せる事実なので，これは一般論で述べておこう.

補題 1　K を n 次代数体とする．正数 $\gamma_1, \cdots, \gamma_n$ が与えられたとき,

$$|\omega^{(i)}| \leqq \gamma_i \quad (i = 1, 2, \cdots, n)$$

を満たす $\omega \in \mathbb{O}_K$ は有限個である.

証明　$\omega_1, \cdots, \omega_n$ を K の整数基とする．任意の $\omega \in \mathbb{O}_K$ は

$$\omega = x_1\omega_1 + \cdots + x_n\omega_n \quad (x_1, \cdots, x_n \in \mathbb{Z})$$

と表せる．このとき

$$\omega^{(i)} = x_1\omega_1^{(i)} + \cdots + x_n\omega_n^{(i)} \quad (i = 1, 2, \cdots, n)$$

であるから，クラメルの公式によって

$$x_1 = \frac{\omega^{(1)}\Delta_{11} + \omega^{(2)}\Delta_{21} + \cdots + \omega^{(n)}\Delta_{n1}}{\Delta}$$

$$\cdots$$

$$x_n = \frac{\omega^{(1)}\Delta_{1n} + \omega^{(2)}\Delta_{2n} + \cdots + \omega^{(n)}\Delta_{nn}}{\Delta}$$

である．ここに $\Delta = \det(\omega_j^{(i)})$ であり，Δ_{ij} は Δ の (i, j) 余因子である. $|\Delta_{ij}/\Delta|$ の最大値を M とすれば,

$$|x_i| \leqq M(\gamma_1 + \cdots + \gamma_n) \quad (i = 1, \cdots, n)$$

となる．こうした $x_i (\in \mathbb{Z})$ は当然有限個である.　‖

系　$\omega \in \mathbb{O}_K$ が $|\omega^{(i)}| = 1$ $(i = 1, \cdots, n)$ を満たせば，1 の冪根である.

証明　$|\omega^{(i)}| = 1$ を満たす $\omega \in \mathbb{O}_K$ は，補題 1 により，有限個である．一方，ω^k も同じく $|(\omega^k)^{(i)}| = 1$ を満たすので，$\omega^k = \omega^{k'}$ $(k \neq k')$ となる $k, k' (\in \mathbb{N})$ が存在する.　‖

補題 2　ω を与えられた実数とする．各 $n \in \mathbb{N}$ に対して

$$|y - \omega x| < \frac{1}{n},\quad 0 < x \leqq n$$

を満たす $x, y (\in \mathbb{Z})$ が存在する．

証明　区間 $[0,1)$ を n 個の区間

$$\left[0, \frac{1}{n}\right),\ \left[\frac{1}{n}, \frac{2}{n}\right),\ \cdots,\ \left[\frac{n-1}{n}, \frac{n}{n}\right)$$

に分ける．$n+1$ 個の実数 $(\in [0,1))$

$$i\omega - [i\omega],\quad i = 0, 1, \cdots, n$$

を考える (ここに $[x]$ は x を超えない最大の整数) と，上の小区間は n 個しかないから，少くとも一つの小区間に 2 個の実数 $i\omega - [i\omega]$ が入る．(これが有名な**ディリクレの部屋割論法**である．) それらを

$$r\omega - [r\omega],\quad s\omega - [s\omega]$$

としよう．そして $r - s = a$, $[r\omega] - [s\omega] = b$ と置こう．明らかに

$$|(r\omega - [r\omega]) - (s\omega - [s\omega])| < \frac{1}{n}$$

$$\therefore\quad |a\omega - b| < \frac{1}{n}$$

$r \neq s$ だから $a \neq 0$ かつ $|a| \leqq n$．‖

この補題を $\left|\omega - \dfrac{y}{x}\right| < \dfrac{1}{nx}$ と変形すると実数 ω を有理数で近似する度合いを表していることがわかるが，この話題にはここでは触れない．

補題 3　実 2 次体 $K = \mathbb{Q}(\sqrt{m})$ には ± 1 ではない単数が存在する．

証明　補題 2 によって

$$|a_1 - b_1\sqrt{m}| < \frac{1}{n_1},\quad 0 < b_1 \leqq n_1$$

となる $a_1, b_1 (\in \mathbb{N})$ が取れる．$a_1 - b_1\sqrt{m} \neq 0$ だから

$$\frac{1}{n_2} < |a_1 - b_1\sqrt{m}|$$

なる $n_2 (\in \mathbb{N})$ が存在する．そして

$$|a_2 - b_2\sqrt{m}| < \frac{1}{n_2},\quad 0 < b_2 \leqq n_2$$

となる $a_2, b_2 (\in \mathbb{N})$ が取れる．かくして

$$\frac{1}{n_{i+1}} < |a_i - b_i\sqrt{m}| < \frac{1}{n_i}, \quad 0 < b_i \leqq n_i \quad (i = 1, 2, \cdots)$$

となる a_i, b_i, n_i の列が次々取れることになる．(ここでも，また以下でも，無限列である必要はないので選択公理は必要ない．) そこで

$$\alpha_i = a_i - b_i\sqrt{m}$$

と置けば，$\alpha_i \in \mathbb{O}_K$ であって，

$$|\alpha_1| > |\alpha_2| > \cdots$$

が成り立っている．

$$\begin{aligned}|N_K\alpha_i| &= |(a_i - b_i\sqrt{m}) \cdot (a_i + b_i\sqrt{m})| \\ &= |(a_i - b_i\sqrt{m})^2 + 2b_i\sqrt{m}(a_i - b_i\sqrt{m})| \\ &\leqq |a_i - b_i\sqrt{m}|^2 + 2|b_i(a_i - b_i\sqrt{m})|\sqrt{m} \\ &\leqq 1 + 2\sqrt{m} \quad (\text{一定})\end{aligned}$$

ところが $N_K\alpha_i \in \mathbb{N}$ だから

$$N_K\alpha_i = N_K\alpha_j$$

がいくらでも多くの i, j に対して成り立つ．この値を g としよう ($g = N_K\alpha_i$)．

再び部屋割論法によって

$$a_i \equiv a_j \pmod{g}, \quad b_i \equiv b_j \pmod{g} \tag{2}$$

なる相異なる α_i, α_j が存在する．$i < j$ とすると

$$\begin{aligned}\frac{\alpha_j}{\alpha_i} &= \frac{a_j - b_j\sqrt{m}}{a_i - b_i\sqrt{m}} = \frac{(a_j - b_j\sqrt{m})(a_i + b_i\sqrt{m})}{N_K\alpha_i} \\ &= \frac{(a_j a_i - b_j b_i m) + (a_j b_i - a_i b_j)\sqrt{m}}{g}\end{aligned}$$

(2) によって

$$a_j a_i - b_j b_i m \equiv a_i^2 - b_i^2 m = g \equiv 0 \pmod{g}$$

$$a_j b_i - a_i b_j \equiv 0 \pmod{g}$$

となり，$\alpha_j/\alpha_i \in \mathbb{O}_K$，しかも $N_K(\alpha_j/\alpha_i) = 1$，かつ $|\alpha_j/\alpha_i| < 1$．これは $\eta = \alpha_j/\alpha_i$ が ± 1 ではない単数であることを示している． ‖

実2次体の場合には $\Phi : U_K \longrightarrow \mathbb{R}^2$ は

$$\Phi(\varepsilon) = (\log|\varepsilon|, \log|\varepsilon'|)$$

である (ここに ε' は ε の共役数). そして像 $\Phi(U_K)$ は

$$\mathbb{H} = \{(x, y) \mid x + y = 0\}$$

に含まれている. $\mathbb{H}$ は $\mathbb{R}^2$ の1次元の部分空間であるから (補題3で保証された η を取ると)

$$(\log|\eta|, \log|\eta'|)$$

で生成されている. したがって任意の $\varepsilon \in U_K$ は

$$\Phi(\varepsilon) = x\Phi(\eta), \quad x \in \mathbb{R}$$

と表せるはずである. U_K の部分集合

$$T = \{\varepsilon(\in U_K) \mid \Phi(\varepsilon) = x\Phi(\eta), 0 \leqq x \leqq 1\}$$

を考えると, $\varepsilon \in T$ は

$$\log|\varepsilon| = x \log|\eta|$$

$$\log|\varepsilon'| = x \log|\eta'|$$

かつ $0 \leqq x \leqq 1$ なので $\log|\varepsilon|, \log|\varepsilon'|$, したがって $|\varepsilon|, |\varepsilon'|$ は有界である. ここで補題1を適用するとこのような $\varepsilon(\in U_K)$ は有限個しかないことがわかる. そこで上のような x が最小正となる ε を選んで ε_0 とし, $\Phi(\varepsilon_0) = x_0\Phi(\eta)$ とする.

任意の $\varepsilon \in U_K$ を取ると

$$\Phi(\varepsilon) = y\Phi(\eta), \quad y \in \mathbb{R}$$

と表せる. $\mathbb{R}$ を小区間 $[mx_0, (m+1)x_0)$ $(m \in \mathbb{Z})$ で分割すると, y はいずれかの小区間に入るから, $y \in [ax_0, (a+1)x_0)$ とすると

$$ax_0 \leqq y < (a+1)x_0$$

である. 故に

$$\Phi(\varepsilon\varepsilon_0^{-a}) = z\Phi(\eta)$$

ただし z は

$$0 \leqq z = y - ax_0 < x_0$$

を満たすが，x_0 の取り方によって $z = 0$ でなければならない．すなわち $\varepsilon\varepsilon_0^{-a} \in W_K = \{\pm 1\}$ である．

以上によって，任意の $\varepsilon \in U_K$ が $\varepsilon = \pm\varepsilon_0^a$ という形に表せることが証明されたのである．

実2次体の場合だけに制限したのだが，証明の本質はすでによく表れている．補題3のかわりに，一般に

$$|\eta_j^{(i)}| > 1 \ (i = j), \quad |\eta_j^{(i)}| < 1 \ (i \neq j) \tag{3}$$

を満たす単数 $\eta_1, \cdots, \eta_r$ $(r = s + t - 1)$ の存在が保証されれば，$\Phi(\eta_1), \cdots, \Phi(\eta_r)$ は1次独立となり，単数定理の証明は2次体の場合と併行的に進められるのである．((3) という性質を有する単数系 $\eta_1, \cdots, \eta_r$ のことを**ミンコウスキ単数**と呼んでいる．)

第10章　三大作図不能問題など

§1. 三大作図不能問題

体の理論の応用としてギリシア時代から伝えられる作図問題を扱う．

与えられた条件を満足する図形を作ることが「作図」という言葉の定義であるが，決められた作図法しか用いられないという制限を付するとその制限の与え方に応じて種々の問題が生じてくる．古くから「作図」と称しているのはこのうち，

> 定木とコンパスのみを，しかも定木は，与えられた二点を通る直線を引くためだけ，またコンパスは与えられた一点を中心として与えられた半径の円を描くためだけに用いることを許す

という制限を付した作図のことである．(たとえば中心を直線に沿ってスライドさせながらコンパスを用いることは許されない．)　このときギリシアの三大作図 (不能) 問題というのは次のように述べられる：

1. **角の三等分問題**　任意に与えられた角を三等分せよ．

2. **立方倍問題**　与えられた立方体の 2 倍の体積を持つ立方体 (の一辺) を作図せよ．

3. **円積問題**　与えられた円と等しい面積を持つ正方形を作図せよ．

定木とコンパスのみを用いて，という制限を取り去るならば，これらがあ

る種の道具を用いて作図可能なことは紀元前4世紀にはすでに知られていたそうである．1., 3. はその名をこれらの作図問題に由来する「円積曲線」を用いて肯定的に解かれる．円積曲線は代数曲線 (すなわち代数方程式で定義される曲線) ではないが，2. は円の同類にすぎない双曲線と放物線の交点として求められる．その訳はあとで述べる．

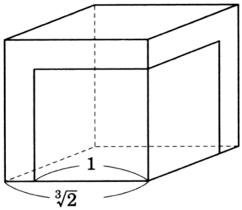
直線と円とが特に簡単に描けるという以外には定木とコンパスだけでなくてはならない理由は見当たらない．直線や円にしたって完全なものは描けるはずもなく，実際に描くという立場からみても直線と円とが特別の立場を主張出来る訳はないのである．(たとえば2定点からの距離の和が一定であるような点の軌跡として楕円が「実際」に描けることに注意しよう.)　したがってかかる制限には本質的意味はないのであるが，なにかしら古代ギリシア人の美意識が感じられるだろう．

ギリシアでは，天体の運動は円軌道であり，それに加えて，流星のような直線運動が二義的に存在すると信じられていた．この思想が作図の手段として定木とコンパスに限定するに至る背景となっているのではないだろうか．

ただこんな本当はあまり本質的ではない制限が歴史的には当然の如くみなされ，そのためにかえって問題がおもしろく感じられ，数多くの人の興味をつないで来た，その結果が体論による説明に人をして耳を傾けせしめるという効果があるということは合理性と人間の思い込みとの関連などについて意味深いものを感ぜしめるのである．

他の例を挙げるなら，代数方程式の解法を冪根に限定する思い込みや不定方程式の整数解への執着が代表的だろう．高次方程式の冪根による解法への執着はまた後に述べることにして，整数解のことで言えば，$x^2 - Dy^2 = 1$ という不定方程式は有理数解ならごく簡単に求まるのに，何故か整数解が問題とされる．またたとえば，$x^3 + y^3 = z^3$ だが，$x = y = 1$, $z = \sqrt[3]{2}$ とすれば解になるが，自然数解に制限することによってきわめて難しい問題が生じるのである．こうした不定方程式の整数解への拘わりは，作図問題と並んで，ギリシア思想が永く影響を及ぼした結果であると言えよう．

さてまずその伝説にちなんでデロスの問題とも呼ばれる立方倍積問題から扱おう．



立方倍積問題

与えられた立方体の一辺の長さを 1 とし，求める立方体の一辺の長さを x とすれば，

$$x^3 = 2 \tag{1}$$

という関係を満たす実数 x が作図されればよいことがわかる．すなわち $x = \sqrt[3]{2}$ である．

円以外の 2 次曲線も使えるとしよう．放物線 $y = x^2$ と双曲線 $xy = 2$ とを描くと，その交点の x 座標がちょうど $\sqrt[3]{2}$ であるから $\sqrt[3]{2}$ が作図されたことになる．だから，円と直線に限定するのでなければ何もおもしろくないのである．

次に円積問題を考えよう．半径 1 の円の面積は π である．したがって求める正方形の一辺の長さを x とすれば

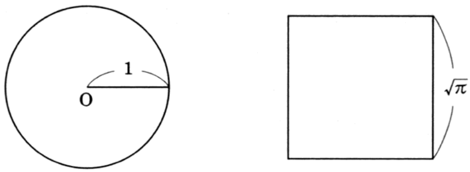
$$x^2 = \pi \tag{2}$$

である．つまり「1 を知って π を知れ (作図せよ)」という問題である．

最後に角の三等分を考える．一例として，与えられた角が $\pi/3$ (すなわち $60°$) であるとする．

その 1/3 の角度は $\pi/9$ で，三角関数の 3 倍角の公式によって

$$\cos\frac{\pi}{3} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}$$

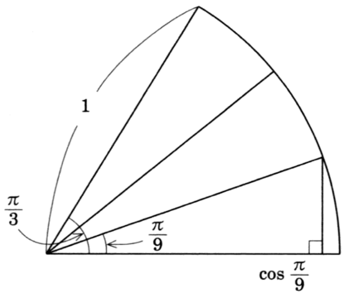


円積問題

そこで $x = 2\cos\dfrac{\pi}{9}$ と置くと，$\cos\dfrac{\pi}{3} = \dfrac{1}{2}$ だから

$$x^3 - 3x - 1 = 0 \tag{3}$$

を得る．かりに x が作図できるならば $\cos\dfrac{\pi}{9}$ も作図でき，したがって $\dfrac{\pi}{9}$ も作図できることになる．



角の三等分問題

以上によって作図問題 1., 2., 3. は (1), (2), (3) の各 x が定木とコンパスでは作図出来ないことを示せば否定的に解決されたことになるのである．

問題　$x^3 - 3x - 1$ は $\mathbb{Q}[x]$ において既約なことを示せ．

[ヒント]　可約とすればその因子の少なくとも一つは 1 次式である．

いま平面上に直交軸を引き，与えられた点にはその座標を，与えられた角

にはその正弦，余弦を，そして与えられた円にはその中心の座標と半径を対応させる．かくして与えられた情報はいくつかの実数 $\alpha_1, \cdots, \alpha_n$ を与えることに帰着される．有理数体 $\mathbb{Q}$ に $\alpha_1, \cdots, \alpha_n$ を添加した実数体 $\mathbb{R}$ の部分体を K と記す：

$$K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$$

いま K_j が実数体の部分体であるとし，2 点 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ は $x_i, y_i \in K_j$ $(i = 1, 2)$ なる点とする．こういう点を K_j 点と呼ぼう．直線 PQ は

$$(y_1 - y_2)x + (x_2 - x_1)y + (x_1 y_2 - x_2 y_1) = 0 \tag{4}$$

と表せる．(4) の係数はすべて K_j の元である．このような型の 2 直線の交点は再び K_j 点である．

次に K_j 点 (x_0, y_0) を中心とし，半径 r $(\in K_j)$ なる円は

$$(x - x_0)^2 + (y - y_0)^2 = r^2 \tag{5}$$

と表せる．(4) と (5) の型の直線との交点を (α, β) とすると (α, β) は K_j 点であるか，または K_j 上の 2 次体 $K_{j+1} = K_j(\sqrt{\theta}), \theta \in K_j$ を適当に取れば K_{j+1} 点である．

同様に (5) 型の 2 円の交点も K_j 点であるか，K_j 上のある 2 次体 K_{j+1} を取ると K_{j+1} 点となる．(5) 型の 2 式の差は 1 次式になるからである．

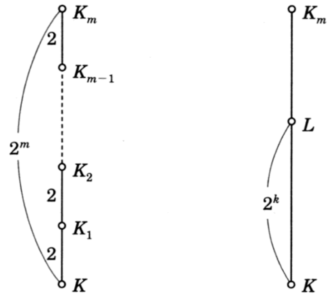
最後に P, Q が K_j 点であるとき P, Q の距離 $\overline{PQ}$ も K_j の元であるか，ある 2 次体 K_{j+1} に対して $\overline{PQ} \in K_{j+1}$ となる．

以上の作業を繰り返して行って 2 次拡大を得る回数を m とすれば体の列

$$K = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_m, \quad [K_{j+1} : K_j] = 2$$

が得られ，作図上現れる点の座標はすべて K_m に属することになる．

そのとき，果たして $[K_m : K] = 2^m$ となるであろうか．そしてまた L が K と K_m の中間体，すなわち $K \subsetneqq L \subsetneqq K_m$ であれば $[L : K]$ は $[K_m : K]$ の約数であろうか．(F が K の拡大体のとき $[F : K]$ によって F を K 上のベクトル空間とみなした際の F の K 上の次元を表すのであった．)



仮りにこれらのことが正しいならば，たとえば立方倍積問題はたちまち否定的に解決されてしまう．なぜなら体

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

では $1, \sqrt[3]{2}, \sqrt[3]{4}$ が $\mathbb{Q}(\sqrt[3]{2})$ の $\mathbb{Q}$ 上の基底となり ($x^3 - 2$ が $\mathbb{Q}$ 上既約だからである)，したがって $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ がわかる．ところが与えられた情報は単位の長さ 1 だけだから $K = \mathbb{Q}$，したがって $\sqrt[3]{2}$ が定木とコンパスで作図できるとすると $\sqrt[3]{2}$ が $\mathbb{Q}$ 上の 2 の冪次拡大体 L の元ということになる．すなわち $\mathbb{Q}(\sqrt[3]{2}) \subseteqq L$．これは次の定理に矛盾する．

定理 10.1 (拡大次数の連鎖律)　M を K の拡大体，L を M の拡大体とする．L が K 上有限次の拡大であれば

$$[L : K] = [L : M][M : K]$$

が成り立つ．

証明　L の M に関する基底を $\{\alpha_1, \cdots, \alpha_m\}$，ここに $m = [L : M]$，また M の K に関する基底を $\{\beta_1, \cdots, \beta_n\}$，ここに $n = [M : K]$ とすれば mn 個の元 $\{\alpha_i\beta_j \mid 1 \leqq i \leqq m, 1 \leqq j \leqq n\}$ が L/K の基底となる．したがって $[L : K] = mn = [L : M][M : K]$．　‖

問題　上の証明で $\{\alpha_i\beta_j \mid 1 \leqq i \leqq m, 1 \leqq j \leqq n\}$ が L の K に関する基

底であることを詳しく証明せよ．

[ヒント]　L の元はすべて $\sum_{i,j} x_{ij}\alpha_i\beta_j (x_{ij} \in K)$ の形に表されること，および $\sum_{i,j} x_{ij}\alpha_i\beta_j = 0 (x_{ij} \in K)$ より $x_{ij} = 0 (\forall i\ \forall j)$ を示せばよい．

これで立方倍積問題が否定的に解決された．同様に (3) を満足する x ($\in \mathbb{R}$) を $\mathbb{Q}$ に添加した体 $\mathbb{Q}\left(\cos\dfrac{\pi}{9}\right)$ は $\mathbb{Q}$ 上 3 次であるから $\dfrac{\pi}{3}$ を 3 等分する作図は不可能なことがわかる．

残ったのは円積問題である．本書では説明しないが，π は代数的数ではない．(こういう数は超越数と呼ばれている．)

したがって $\sqrt{\pi}$ も同様に超越数である．したがって当然のことながら $\mathbb{Q}$ の 2 の冪次の拡大体には含まれない．

ギリシアの三大作図問題はデカルトも著書『幾何学』(1637 年) の中で扱っているが，著書の精神をわきまえれば容易に解決が着くとして，読者に任されている．たとえば $\sqrt[3]{2}$ は

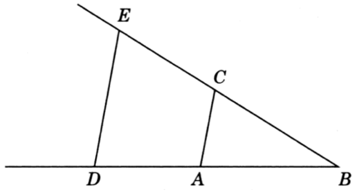
$$\sqrt[3]{2} = \sqrt{\sqrt{a} + \sqrt{b}} + \sqrt{\sqrt{c} - \sqrt{d}}$$

とでもいった平方根を重ねることで表されそうにないことは直感的には予想されるが，その証明は容易ではない．立方倍積問題，角の三等分問題は数学史的には，19 世紀に解決されたことになっているけれども，おそらく現代の批判的目に耐えるような証明ではないのではないかという気がする．厳密に言えば，やはり体論の登場によって解決されたと評価すべきではなかろうか．

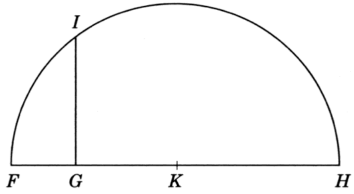
ところで三大作図不能問題は否定的解決だから，3 次方程式の根は作図できないということですむが，では作図可能なものは何かという問題を解決しておこう．

次の図はデカルトの『幾何学』からの引用である：

$AB = 1, BD = a, BC = b$ とすると比例関係によって $BE = a \cdot b$ となる．ここでは，2 数の積を示したが，和・差・商も同様に作図できる．したがって，1 という単位が与えられると，任意の有理数が作図可能である．



また次の図も『幾何学』からの引用である：



これは α という正数が与えられているとき $\sqrt{\alpha}$ も作図可能であることを示している．$GH = \alpha, FG = 1, K$ を FH の中点とすれば $GI = \sqrt{\alpha}$ である．つまり体 K の元が作図可能なら $K(\sqrt{\alpha}), \alpha \in K$ の元も作図可能である．

以上によって，$\alpha_1, \cdots, \alpha_n$ を与えられた情報を表す値として，

$$K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$$

を $\mathbb{Q}$ にこれらを添加した体とする．そして

$$K = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_{m-1} = K_m, \quad [K_{j+1} : K_j] = 2$$

なる体の列を作れば，K_m の元となる数はすべて作図可能となるということが結論できる．

§ 2. 代数方程式を解くとは？

$\sqrt{a}$ との類似で $\sqrt[3]{2}$ などが考え出されたが，任意の 3 次方程式が「代数的に解ける」こと，すなわち方程式の係数と $\sqrt{\ }$，$\sqrt[3]{\ }$ の記号の組み合わせで解が表せることが証明されたのは 16 世紀になってからであった．2 次方程式

$$x^2 + ax + b = 0$$

は

$$\left(x + \frac{a}{2}\right)^2 + \frac{4b - a^2}{4} = 0$$

と変形できるから平方根の記号で足りるのは当然だが，3 次方程式

$$x^3 + ax^2 + bx + c = 0 \tag{6}$$

は $X = x + \dfrac{a}{3}$ の変換によっても

$$X^3 - 3AX + B = 0 \tag{7}$$

の形にしか変形できないのだから，それが A, B と $\sqrt{\ }$，$\sqrt[3]{\ }$ の記号の組み合わせだけで解けてしまうのは，なんだか不思議な気がする．

問題 $x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x + y\omega + z\omega^2)(x + y\omega^2 + z\omega)$ (ここに，$\omega^2 + \omega + 1 = 0$ とする) という因数分解を示し，これを用いて，3 次方程式 (7) を解け．

[ヒント] $x^3 + y^3 + z^3 - 3xyz = x^3 - 3yzx + (y^3 + z^3)$ と考え，$yz = A, y^3 + z^3 = B$ から y, z を求めればよい．

誰が考えついたのか知らないが，

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx)$$

とはまたすごい因数分解である．こんなのは発見者の人名を冠して顕彰すべきではなかろうか．

3 次方程式の解が冪根の記号で表現できることだけでもオドロキなのに，4 次方程式まで次のように代数的に解けてしまうのである．

問題 $x^4 + ax^2 + bx + c = (x^2 + kx + \ell)(x^2 - kx + m)$

と置き，k, ℓ, m と a, b, c の関係を求めることによって 4 次方程式の代数的解法の流れを定めよ．

問題　上の方法によって次の 4 次方程式を解け：

$$x^4 - 4x^3 - x^2 + 10x + 6 = 0$$

しかし無論このような幸運がいつまでも続くはずもなく，$x^n = a$ の解にすぎない $\sqrt[n]{a}$ の四則でもって高次方程式が解けてしまうという茶番劇は，よくご承知の通り，19 世紀初頭に終幕を迎えたのであった．すなわちアーベルによって次の定理が証明されたのである (証明は第 12 章で与える)：

定理 10.2 (アーベル)　一般 5 次方程式は代数的に解けない．

作図においては円だけを特待生扱いしたのと同じような固定観念が，方程式においては冪根だけを特別に扱い，一般の解までも支配できるはずだとする，今から考えると不思議なような固定観念が数学を支配したのであった．

中世においては，2 次の無限数だけが手の届く無理数であったのと同じように，幾何学的には円，代数的には 2 次方程式だけが (感性的にまでも) 手の届く考察の対象であったのではなかろうか．

アーベルの定理を証明するにはガロアの理論が必要であるから証明は次章以降に与える．

一方，有理数や $\sqrt{2}$ などの小数展開から始まって無限小数の全体といったゴツイ代物を考察することによって実数体 $\mathbb{R}$ ができ上がる．そして逆にこれによって直線のイメージが現在読者が抱いているようなものとして確定するのである．

アーベルの定理で知られるように $\sqrt{2}$ や $\sqrt[3]{5}$ といった冪根で表せる数の全体と代数的数全体とでは大きなギャップがあるが，実数全体と実数の代数的数の全体とではさらに大きなギャップがある．発生の系統を異にしているのだからこれは別に不思議なことではない．にもかかわらず，永い間数とは方程式の根となるもののことであり，それはいずれ冪根で表されるものと信じられていたのである．

第11章　代数体のイデアル論

§1. 素イデアル分解

代数体 K の整数環 $\mathbb{O}_K$ においては，一般には一意的な素元分解が可能ではない．つまり $\mathbb{O}_K$ が U.F.D. ではないような代数体が存在する．そこで考え出されたのがイデアルという概念である．本書では特に断らない限り $\{0\}$ ではないイデアルのみを扱う．

本節の目標は次の命題を証明することである：

定理 11.1 (代数体のイデアル論の基本定理) $\mathfrak{A}$ を $\mathbb{O}_K$ の任意のイデアルとすると

$$\mathfrak{A} = \mathfrak{P}_1^{n_1} \cdots \mathfrak{P}_s^{n_s}$$

というように相異なる素イデアルの冪積に分解でき，しかもこのような分解は順序を除けば一意的である．

まずイデアルの積を定義しておかねばならない．

定義 A, B を環 R のイデアルとするとき，その積 AB を A の元 α と B の元 β の積 $\alpha\beta$ をすべて含むような R のイデアルとする．即ち

$$AB = \left\{ \sum_j x_j \alpha_j \beta_j \mid x_j \in R, \alpha_j \in A, \beta_j \in B \right\}$$

ここに $\sum_j$ は任意個の有限和を表す．

R が P.I.D. の場合，$A = (\alpha), B = (\beta)$ とすると $AB = (\alpha\beta)$ となるから，上の定理は P.I.D. における一意的素因数分解性の一般化になっていることがわかるだろう．

イデアルの起源を述べると次のようである．フェルマー方程式

$$x^\ell + y^\ell = z^\ell$$

に自然数解があるとすると，ζ を 1 の原始 ℓ 乗根として，$\mathbb{Z}[\zeta]$ において

$$(x+y)(x+\zeta y)\cdots(x+\zeta^{\ell-1}y) = z^\ell$$

となる．仮りに左辺の因子がそれぞれ互いに共通因子を含まないなら

$$(x+\zeta^j y) = \mathfrak{A}_j^\ell \quad (\mathfrak{A}_j \text{ は } \mathbb{Z}[\zeta] \text{ のイデアル})$$

と表せることになる (定理 11.1)．そして K が (イデアル類群の位数が ℓ と素といった) ある種の条件を満たせば

$$\mathfrak{A}_j = (A_j)$$

となる $A_j \in \mathbb{O}_K$ が取れて

$$x + \zeta^j y = \varepsilon_j A_j^\ell \quad (\varepsilon_j \text{ は } K \text{ の単数})$$

と書けることになる，というような道筋をたどってフェルマー予想が上記のようなある条件のもとに解決されるのである．これが本格的な代数的整数論の発祥の場面であり，同時にイデアル論，ないしは因子論誕生の場面でもあるわけである．

定理 11.1 を証明するためにいくつかのステップを用意する．

極大条件　$\mathbb{O}_K$ のイデアルの集合 S が与えられると，S の中では包含関係について極大なものが存在する．すなわち $\forall A \in S\ (M \subseteq A \Rightarrow M = A)$ を満たす $M \in S$ が存在する．

証明　$0 \neq a \in \mathfrak{A}$ なる自然数 a を取ると $(a) = \mathbb{O}_K a \subseteqq \mathfrak{A}$ である．$\omega_1, \cdots, \omega_n$ を $\mathbb{O}_K$ の整数基とすると

$$(a) = \mathbb{Z}a\omega_1 + \cdots + \mathbb{Z}a\omega_n \quad (\text{直和})$$

である．故に

$$\mathbb{O}_K/(a) \simeq \mathbb{Z}/\mathbb{Z}a \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}a$$

$\therefore$ $|\mathbb{O}_K/(a)| = a^n < \infty$．つまり $\mathbb{O}_K/(a)$ は有限加群であるので $\mathbb{O}_K/\mathfrak{A}$ も同様である．したがって $\mathfrak{A} \subseteqq \mathfrak{B}$ なるイデアル $\mathfrak{B}$ は有限個しか存在しない．
‖

素イデアルの極大性　$\mathbb{O}_K$ の素イデアルは極大イデアルである．

証明　$\mathfrak{P}$ を素イデアルとすると $\mathbb{O}_K/\mathfrak{P}$ は整域であり，しかも有限集合であるから必然的に体をなす．故に $\mathfrak{P}$ は極大イデアルである．‖

整閉性　$\alpha \in K$ に対して

$$\lambda\alpha^n \in \mathbb{O}_K \quad (n = 0, 1, 2, \cdots)$$

となる $\lambda \in K^\times$ が存在するなら，$\alpha \in \mathbb{O}_K$ でなければならない．

証明　イデアル $\mathfrak{A}_n$ を $\mathfrak{A}_n = (\lambda, \lambda\alpha^2, \cdots, \lambda\alpha^n)$ で定義すると

$$\mathfrak{A}_0 \subseteqq \mathfrak{A}_1 \subseteqq \mathfrak{A}_2 \subseteqq \cdots \subseteqq \mathfrak{A}_n \subseteqq \cdots$$

が成り立つが，極大条件によって $\mathfrak{A}_m = \mathfrak{A}_{m+1}$ となる m が存在する．故に

$$\lambda\alpha^{m+1} = \beta_0\lambda + \beta_1\lambda\alpha + \cdots + \beta_m\lambda\alpha^m \quad (\beta_0, \beta_1, \cdots, \beta_m \in \mathbb{O}_K)$$

と表せる．故に

$$\alpha^{m+1} - \beta_m\alpha^m - \cdots - \beta_1\alpha - \beta_0 = 0$$

である．これは α が代数的整数であることを示しており (次ページの問題参照)，しかも $\alpha \in K$ だから $\alpha \in \mathbb{O}_K$ である．‖

問題　$\alpha \in \mathbb{C}$ が

$$X^{m+1} + \beta_1 X^m + \cdots + \beta_m X + \beta_{m+1} = 0$$

(ここに $\beta_1, \cdots, \beta_{m+1}$ は代数的整数) という形の方程式の根ならば α は代数的整数である．これを示せ．

[ヒント]　定理 7.6 の証明のまねをすればよい．

実は代数体の整数環でなくても上の三つの条件が成り立つ整域なら，素イデアル分解とその一意性が成り立つ．そこで次のように定義する：

定義　極大条件，素イデアルの極大性，整閉性の成り立つ整域を**デデキント整域**と呼ぶ．

一般論のほうが見易いので，以下では D をデデキント整域，K をその商体としよう．D のイデアルを A, B, C 等で表す．以下でもイデアルは $\{0\}$ でないとする．

補題 1　P を D の素イデアルとする．このとき

$$AB \subseteqq P \Longrightarrow A \subseteqq P \text{ または } B \subseteqq P.$$

証明　$\neg(A \subseteqq P)$ かつ $\neg(B \subseteqq P)$ とせよ．すると

$$\exists a \in A; a \notin P \text{ かつ } \exists b \in B; b \notin P$$

であるが，$ab \in AB \subseteqq P$ より $ab \in P$ となる．即ち，$ab \in P$ だが $a \notin P$, $b \notin P$ となり，P は素イデアルではないことになる．‖

補題 2　A を D のイデアルとすると $A \supseteqq P_1 \cdots P_n$ となる有限個の素イデアル $P_1, \cdots, P_n$ が存在する．

証明　決して素イデアルの積を含まないようなイデアルすべての集合を S とし，$S \neq \varnothing$ とする．極大条件によってそういう性質を持つ極大なイデアル

$A \in S$ が存在する．A 自身が素イデアルということはありえないから，

$$b \notin A, \quad c \notin A, \quad bc \in A$$

なる $b, c\ (\in D)$ が存在する．そこで

$$B = A + Db, \quad C = A + Dc$$

と置くと，

$$A \subsetneqq B, \quad A \subsetneqq C, \quad BC \subseteqq A$$

が成り立つ．しかし A の極大性によって B, C は素イデアルの積を含む．したがって A も素イデアルの積を含むことになって矛盾を生じる．ゆえに，$S = \varnothing$ である． ‖

定義　素イデアル P に対して

$$P^{-1} = \{x(\in K) \mid xP \subseteqq \mathrm{D}\}$$

と定義する．

このとき，$\mathrm{D} \subseteqq P^{-1}$ は，P がイデアルだから明らかである．P^{-1} の元と P の元の積和の全体を $P^{-1}P$ と記せば，$P^{-1}P \subseteqq \mathrm{D}$ だから，$P^{-1}P$ は D のイデアルをなすことがわかる．$P \subseteqq P^{-1}P \subseteqq \mathrm{D}$ だが，P は素イデアルと仮定しているから極大イデアルでもあるので

$$P^{-1}P = P \text{ または } P^{-1}P = \mathrm{D}$$

のいずれかが成り立つ．

補題 3　素イデアル P に対して

$$P^{-1}P = D$$

証明　仮りに $P^{-1}P = P$ とすると，任意の n に対して

$$(P^{-1})^n P = P \subseteqq \mathrm{D}$$

となる．したがって任意に $\alpha \in P^{-1}$ を取り，$0 \neq \pi \in P$ とすると

$$\pi\alpha^n \in \mathrm{D} \quad (n = 0, 1, 2, \cdots)$$

を得るが D の整閉性によって $\alpha \in \mathrm{D}$ となる．故に $P^{-1} \subseteqq \mathrm{D}$ である．

したがって，$P^{-1} \supsetneqq \mathrm{D}$ が示せれば矛盾を生じ，$P^{-1}P = \mathrm{D}$ が証明されたことになる．$0 \neq \pi \in P$ を取る．$(\pi) \supseteqq P_1 \cdots P_m$ となる素イデアルの積のうち，素イデアルの個数 m が最小となるものを選ぶ．$P \supseteqq P_1 \cdots P_m$ 故，補題 1 から，例えば $P \supseteqq P_1$．素イデアルの極大性によって $P = P_1$ となる．ところで

$$(\pi) \supseteqq P_1 \cdots P_m,\ \text{but}\ \neg((\pi) \supseteqq P_2 \cdots P_m)$$

が m の最小性からわかる．そこで $\gamma \in P_2 \cdots P_m$，$\gamma \notin (\pi)$ なる γ を取ると $\dfrac{\gamma}{\pi} \notin \mathrm{D}$ であって

$$\frac{\gamma}{\pi} \cdot P = \frac{1}{\pi} \cdot \gamma P_1 \subseteqq \frac{1}{\pi} P_1 \cdots P_m \subseteqq \mathrm{D}$$

$$\therefore \quad \frac{\gamma}{\pi} \in P^{-1} \qquad \therefore \quad \mathrm{D} \subsetneqq P^{-1}.$$

以上によって，補題 3 が証明された．‖

さて，以上でデデキント整域 D では素イデアル分解とその一意性が成り立つことの証明の準備が整った．

まず分解の可能性を示す．素イデアルの積に表せないイデアルがあるとして，それらの集合 S を考えると極大条件によって S における極大なイデアル A が存在することになる．この A は素イデアルではないから，極大イデアルでもない．したがって $A \subsetneqq P \subsetneqq D$ なる極大イデアル P が存在する (極大条件による)．また $A \subseteqq AP^{-1} \subseteqq D$ だが，補題 3 の証明と同様にして $AP^{-1} \neq A$ が示される．再び A の極大性によって $C = AP^{-1}$ は素イデアル分解が可能である．$A = PC$ だから A 自身が素イデアル分解可能となって矛盾を生じ，$S = \varnothing$ であることが証明された．

分解の一意性は簡単である．即ち

$$P_1 \cdots P_m = Q_1 \cdots Q_n \tag{1}$$

とし，P_i, Q_j は素イデアルとせよ．$P_1 \supseteqq Q_1 \cdots Q_n$ だから，補題 1 よりたとえば $P_1 \supseteqq Q_1$ となるが，共に極大イデアルでもあるから $P_1 = Q_1$ でなけれ

ばならない．(1) の両辺に $P_1^{-1}=Q_1^{-1}$ をかければ

$$P_2\cdots P_m=Q_2\cdots Q_n$$

を得て，これを進めれば分解の一意性が従うのである．

定理 11.2　デデキント整域のイデアルに対しては

$$A\subseteqq B\Longleftrightarrow \exists C;\ A=BC$$

が成り立つ．

この定理も P.I.D. では自明のことだったが，一般のデデキント整域のイデアルではそう容易に示せることではないのである．今後，P.I.D. におけると同様，$A\subseteqq B$ のとき $B|A$ と記すことにしよう．

証明 (定理 11.2 **の証明)**　$A\subseteqq B$ とし $A=P_1\cdots P_m$，$B=Q_1\cdots Q_n$ をそれぞれの素イデアル分解とせよ．

$$P_1\cdots P_m\subseteqq Q_1$$

より，たとえば $P_1=Q_1$ を得る．故に

$$P_2\cdots P_m\subseteqq Q_2\cdots Q_n$$

同様の操作は n 回続けられるので結局 A, B は

$$A=P_1^{a_1}\cdots P_\nu^{a_\nu},\quad B=P_1^{b_1}\cdots P_\nu^{b_\nu},\quad 0\leqq b_i\leqq a_i\ (i=1,\cdots,\nu)$$

というように素因子分解されることがわかるだろう．そこで

$$C=P_1^{a_1-b_1}\cdots P_\nu^{a_\nu-b_\nu}$$

と置けば $A=BC$ を得る．逆は証明するまでもない．　‖

定義　A, B をデデキント整域 D のイデアルとし，

$$A=\prod_i P_i^{a_i},\quad B=\prod_i P_i^{b_i}\qquad a_i\geqq 0,\ b_i\geqq 0$$

をそれぞれの素イデアル分解とする．

$$\prod_i P_i^{\min\{a_i,b_i\}},\quad \prod_i P_i^{\max\{a_i,b_i\}}$$

をそれぞれ A, B の**最大公約イデアル**，**最小公倍イデアル**という．

この定義は自然数の場合の最大公約数，最小公倍数の定義と整合的で納得がいくであろう．ただし最大・最小といっても素因子の個数についての話であって，集合としては逆である．たとえば $A \subseteqq C$, $B \subseteqq C$ なるイデアル C のうちで最小のイデアルが最大公約イデアルである．

命題　A, B の最大公約イデアルは $A + B = \{x + y \mid x \in A, y \in B\}$ であり，最小公倍イデアルは $A \cap B$ である．

証明　$A \subseteqq A + B$, $B \subseteqq A + B$ だから定理 11.2 によって $A + B$ は確かに A, B の公約イデアルである．次に C を A, B の公約イデアルとすると，

$$A \subseteqq C,\ B \subseteqq C$$

だから $A + B \subseteqq C$ である．したがって $A + B$ は A, B の最大公約イデアルである．

次に $A \cap B \subseteqq A$, $A \cap B \subseteqq B$ だから $A \cap B$ は A, B の公倍イデアルである．C を A, B の公倍イデアルとすると $C \subseteqq A$, $C \subseteqq B$ が成り立つので，$C \subseteqq A \cap B$ を得る．即ち $A \cap B$ は最小公倍イデアルである．∥

最大公約イデアルを整数の場合と同様の記号で

$$(A, B)$$

と表す．

$$(A, B) = 1$$

は $(A, B) = (1) = \mathrm{D}$ の意味で，A と B とは互いに素であると言われる．

系　次が成り立つ．

$$(A, B) = 1 \iff \exists a \in A\ \exists b \in B;\ a + b = 1 \tag{2}$$

また

$$(A, B) = 1 \iff A \cap B = AB.$$

(2) が $\mathbb{Z}$ における

$$(a,b)=1 \iff \exists x,y\in\mathbb{Z};\ ax+by=1$$

という命題の一般化であることは明らかである．

以上の諸命題によってイデアルという概念が自然数における「倍数」，「約数」という関係を一般のデデキント整域 (とくに代数体) で表現する実にたくみな装置であることが理解されたであろう．類似性の例として孫子の定理 (CRT) を挙げておこう：

定理 11.3 (孫子の定理)　$A_1,\cdots,A_m$ を D のイデアルとし，$(A_i,A_j)=1$ $(i\neq j)$ であるとする．D の元 $\alpha_1,\cdots,\alpha_m$ に対して連立 1 次合同式

$$\begin{cases} x \equiv \alpha_1 & \pmod{A_1} \\ \quad\vdots & \\ x \equiv \alpha_m & \pmod{A_m} \end{cases}$$

は解を持ち，積 $A_1\cdots A_m$ を法として一意的である．

証明　$B_i=A_1\cdots A_{i-1}A_{i+1}\cdots A_m$ と置くと，$(A_i,B_i)=1$ なので $\lambda_i+\mu_i=1$ を満たす $\lambda_i\in A_i$, $\mu_i\in B_i$ が存在する．$j\neq i$ ならば $B_i\subsetneqq A_j$ だから，$\mu_i\in A_j$ である．そこで

$$\xi=\alpha_1\mu_1+\cdots+\alpha_m\mu_m$$

と置くと，

$$\begin{aligned} \xi &\equiv \alpha_1\mu_1 \pmod{A_1}\ \ (\because \mu_i\in A_1\ (i\geqq 2)) \\ &\equiv \alpha_1 \pmod{A_1}\ \ (\because \lambda_1\in A_1) \end{aligned}$$

同様にして，$\xi\equiv\alpha_i \pmod{A_i}$ が成り立つから ξ は連立合同式の解である．

一意性の証明は読者のチェックに任せる．‖

系　A,B を互いに素な D のイデアルとすると環の同型

$$\mathrm{D}/AB\simeq \mathrm{D}/A\oplus \mathrm{D}/B$$

が成り立つ．同型対応は $x \bmod AB \rightsquigarrow (x \bmod A,\ x \bmod B)$ によって与えられる．

証明は標準的な写像 $\mathrm{D} \longrightarrow \mathrm{D}/A \oplus \mathrm{D}/B$ に準同型定理を適用すればよい．このとき $A \cap B = AB$ に注意．

分数イデアルについて　せっかく逆イデアル P^{-1} を導入したのだから分数イデアルという概念も定義しておこう．

デデキント領域 D の商体 K の D 部分加群 A が**分数イデアル**であるとは，αA が D のイデアルとなるような $\alpha(\neq 0) \in D$ が存在することを言う．ここに $A \subsetneqq K$ が D 部分加群であるとは A が K の部分加群であって，さらに

$$xa \in A \quad (\forall x \in D, \forall a \in A)$$

が満たされることである．今までのイデアルは，分数イデアルと区別するためには**整イデアル**と言う．

たとえば有理整数環 $\mathbb{Z}$ とその商体 $\mathbb{Q}$ の例で言えば，$I = \{3x/2 \mid x \in \mathbb{Z}\}$ は $2I = (3)$ なので，分数イデアルである．

さて，一般論に戻って，A が分数イデアルなら，定義によって αA がイデアルとなる $\alpha \neq 0$ が取れる．αA と $(\alpha) = \alpha D$ との素イデアル分解を

$$\alpha A = P_1 \cdots P_s, \qquad (\alpha) = Q_1 \cdots Q_t$$

とせよ．$\alpha A = (\alpha)A$ であるから，

$$A = P_1 \cdots P_s Q_1^{-1} \cdots Q_t^{-1}$$

を得る．そこで，$k > 0$ に対して $P^{-k} = (P^{-1})^k$ と表すことにして，上の式を整理すれば，次の定理が証明されたことになる：

定理 11.4　デデキント整域においては, 任意の分数イデアルは素イデアルの (負の指数まで込めた) 冪積として一意的に表すことができる．言い換えれば，分数イデアルの全体は素イデアルの全体を基底とするアーベル群をなす．

なお，$A = P_1^{r_1} \cdots P_m^{r_m}$ $(r_i \in \mathbb{Z})$ とすれば，A の逆元は $P_1^{-r_1} \cdots P_m^{-r_m}$ だが，これがちょうど $A^{-1} = \{x\,(\in K) \mid xA \subseteq D\}$ と一致することも容易に示せることである．A^{-1} を A の逆イデアルと呼ぶ．

§2. イデアルを法とする剰余環

K を n 次代数体，$\mathbb{O}_K$ をその整数環とする．$\mathfrak{A}$ (A のドイツ文字) を K の (0) でも (1) でもない整イデアルとする．商環，あるいは剰余環 $\mathbb{O}_K/\mathfrak{A}$ について基本的な性質を調べていこう．当然のことながら，$\mathbb{Z}/m\mathbb{Z}$ の性質がどの程度保存されているかが興味あるところである．

基本に戻って，まず，$\alpha, \beta \in \mathbb{O}_K$ に対して $\alpha - \beta \in \mathfrak{A}$ のとき，α と β は mod $\mathfrak{A}$ で合同であるといって

$$\alpha \equiv \beta \pmod{\mathfrak{A}}$$

と記すのであった．この同値関係を使って $\mathbb{O}_K$ を類別し，類 $\alpha \bmod \mathfrak{A} = \{\beta(\in \mathbb{O}_K) \mid \beta \equiv \alpha \pmod{\mathfrak{A}}\}$ の全体 $\mathbb{O}_K/\mathfrak{A}$ に $\mathbb{O}_K$ の演算を遺伝させて，環とするのである．$\alpha \bmod \mathfrak{A}$ のことを $\overline{\alpha}$ と書くことも多い．とくに $\overline{0} = \mathfrak{A}$ である．

命題　$\mathbb{Z} \cap \mathfrak{A}$ は $\mathbb{Z}$ の (0) でも (1) でもないイデアルをなす．

証明　$\alpha(\neq 0) \in \mathfrak{A}$ を一つ取る．α の満たす既約なモニック方程式を考えると

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0, \quad a_1, \cdots, a_n \in \mathbb{Z}$$

であるが，$\mathfrak{A}$ がイデアルであることによって $a_n \in \mathfrak{A}$ がわかり，さらに既約に取ったから $a_n \neq 0$ である．また α は単数ではないので $a_n \neq \pm 1$. $\therefore$ $\mathfrak{A} \cap \mathbb{Z} \neq (0), (1)$．これがイデアルをなすことはすぐにわかる．‖

$\mathbb{Z} \cap \mathfrak{A} = (m)$ とすると，$x \bmod m \rightsquigarrow x \bmod \mathfrak{A}$ によって写像 $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{O}_K/\mathfrak{A}$ が定義されるが，これが 1 対 1 の準同型写像であることは容易に見

て取れることである．つまり，$\mathbb{O}_K/\mathfrak{A}$ は $\mathbb{Z}/m\mathbb{Z}$ を部分環として含んでいると考えてよい．mod $\mathfrak{A}$ の有理整数で代表される類の全体が $\mathbb{Z}/m\mathbb{Z}$ と同一視されるのである．

命題　$\mathbb{O}_K/\mathfrak{A}$ は有限環である．その位数を $\mathfrak{A}$ の**ノルム** (後に導入される，相対ノルムと区別する必要があるときは，**絶対ノルム**) と言って $N_K\mathfrak{A}$ で示す：

$$N_K\mathfrak{A} = (\mathbb{O}_K : \mathfrak{A})$$

証明　$\mathbb{Z} \cap \mathfrak{A} = (m)$ なる $m \in \mathbb{Z}$ を取ると $m\mathbb{O}_K \subseteqq \mathfrak{A}$ である．$\omega_1, \cdots, \omega_n$ を K の整数基とすると

$$m\mathbb{O}_K = \mathbb{Z}m\omega_1 \oplus \cdots \oplus \mathbb{Z}m\omega_n \text{ (直和)}$$

であることは明らかである．

$$\begin{aligned} \mathbb{O}_K/m\mathbb{O}_K &= (\mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n)/(\mathbb{Z}m\omega_1 \oplus \cdots \oplus \mathbb{Z}m\omega_n) \\ &\simeq (\mathbb{Z}/m\mathbb{Z})^n \quad (n \text{ 個のコピー}) \end{aligned}$$

故に，$m > 1$ と取って置けば $(\mathbb{O}_K : m\mathbb{O}_K) = m^n < \infty$. $\mathbb{O}_K \supseteqq \mathfrak{A} \supseteqq m\mathbb{O}_K$ だから $(\mathbb{O}_K : \mathfrak{A}) \leqq m^n$ (実際は m^n の約数)．∥

$(\mathfrak{A}, \mathfrak{B}) = 1$ のとき $N_K\mathfrak{A}\mathfrak{B} = N_K\mathfrak{A} \cdot N_K\mathfrak{B}$ が成り立つことは前節の結果 (定理 11.3 の系) から明らかである．

とくに素イデアル $\mathfrak{p}$ の場合は $\mathbb{O}_K/\mathfrak{p}$ は有限整域となるので，実は体である．$\mathbb{Z} \cap \mathfrak{p} = (p)$ とすると，p は素数である．$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subseteqq \mathbb{O}_K/\mathfrak{p}$ なので，$\mathbb{O}_K/\mathfrak{p}$ は $\mathbb{F}_p$ 上の有限次拡大である．その拡大次数を f と書けば $N_K\mathfrak{p} = |\mathbb{O}_K/\mathfrak{p}| = p^f$ である．この f のことを $\mathfrak{p}$ の**相対次数**と呼ぶ習慣である：$f = [\mathbb{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$

$\mathbb{O}_K/\mathfrak{p}$ の $\overline{0}$ 以外の元のなす群 $(\mathbb{O}_K/\mathfrak{p})^\times$ は以前示したとおり (定理 8.2 の系)，巡回群である．

有理整数環 $\mathbb{Z}$ との対比で言えば，$\xi \in \mathbb{O}_K$ に対してフェルマーの小定理の

一般化

$$\xi^{N_K \mathfrak{p}} \equiv \xi \pmod{\mathfrak{p}}$$

が成り立つことも言うまでもあるまい．剰余体 $\mathbb{O}_K/\mathfrak{p}$ が有限体であるという事実は代数的整数論をおもしろく，奥深くしている秘密の一つであろう．

定理 11.5　代数体 K のイデアル $\mathfrak{A}$ が

$$\mathfrak{A} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}$$

と相異なる素イデアルの冪積に分解されるならば

$$N_K \mathfrak{A} = (N_K \mathfrak{p}_1)^{a_1} \cdots (N_K \mathfrak{p}_s)^{a_s}$$

が成り立つ．

証明　前述のように $(\mathfrak{A}, \mathfrak{B}) = 1$ ならば

$$N_K \mathfrak{A}\mathfrak{B} = N_K \mathfrak{A} \cdot N_K \mathfrak{B}$$

だから，まず

$$N_K \mathfrak{A} = N_K \mathfrak{p}_1^{a_1} \cdots N_K \mathfrak{p}_s^{a_s}$$

がわかる．故に一般に $\mathfrak{p}$ を素イデアルとして

$$N_K \mathfrak{p}^a = (N_K \mathfrak{p})^a$$

を証明すればよい．

$$\mathbb{O}_K \supsetneqq \mathfrak{p} \supsetneqq \mathfrak{p}^2 \supsetneqq \cdots \supsetneqq \mathfrak{p}^a$$

という列を考えると

$$(\mathbb{O}_K : \mathfrak{p}^a) = (\mathbb{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \cdots (\mathfrak{p}^{a-1} : \mathfrak{p}^a)$$

なので，

$$\mathfrak{p}^i / \mathfrak{p}^{i+1} \simeq \mathbb{O}_K / \mathfrak{p} \tag{3}$$

が証明されればよいことになる．$i = 1$ のときに示せば十分だろう．$\mathfrak{p}^2 \subsetneqq \mathfrak{p}$ なので $\pi \in \mathfrak{p}$ だが $\pi \notin \mathfrak{p}^2$ なる元 π を取れる．そこで $\alpha \bmod \mathfrak{p}$ に対して $\pi\alpha \bmod \mathfrak{p}^2$ を対応させる写像 $\mathbb{O}_K \longrightarrow \mathfrak{p}/\mathfrak{p}^2$ を考えれば，任意の $\beta \in \mathfrak{p}$ に対して $\pi\xi \equiv \beta \pmod{\mathfrak{p}^2}$ は解 ξ を持つことが $((\pi), \mathfrak{p}^2) = \mathfrak{p}$ によってわかるので，全射である．またその核は $\mathfrak{p}$ だから (3) が証明された．‖

系　K の任意のイデアル $\mathfrak{A}$, $\mathfrak{B}$ に対して

$$N_K\mathfrak{A}\mathfrak{B} = N_K\mathfrak{A} \cdot N_K\mathfrak{B}.$$

§ 3. イデアル類群

本節でも (分数あるいは整の) イデアル $\neq \{0\}$ という仮定を続ける．デデキント整域 D の分数イデアルの全体のなすアーベル群を J とする．単位元は D である．単項分数イデアルの全体 P はその部分群をなす．商群 J/P を**イデアル類群**という．なお，各イデアル類から整イデアルを代表として選べることは，分数イデアルの定義から明らかである．

以上は一般のデデキント環で成り立つ事柄だが，代数体ではさらに次の著しい命題が成り立つ．

定理 11.6　代数体 K のイデアル類群 C_K は有限群である．その位数 h_K を K の**類数**という．

定理の証明の準備にもなるが，ちょうどよい機会だから代数的数のノルムの定義とイデアルのノルムとの関係を与えておこう．

$\mathfrak{A}$ を代数体 K のイデアルとすると，$\mathfrak{A}$ は $\mathbb{O}_K$ の階数 n $(= [K:\mathbb{Q}])$ の自由部分加群だから，基底 $\alpha_1, \cdots, \alpha_n$ を持つ：

$$\mathfrak{A} = [\alpha_1, \cdots, \alpha_n] = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

$\omega_1, \cdots, \omega_n$ を K の整数基とすると

$$\mathbb{O}_K = [\omega_1, \cdots, \omega_n] = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$$

$\alpha_i \in \mathbb{O}_K$ だから

$$\alpha_i = \sum_{j=1}^{n} a_{ij}\omega_j \quad (a_{ij} \in \mathbb{Z})$$

と表せて

$$N_K\mathfrak{A} = (\mathbb{O}_K : \mathfrak{A}) = |\det(a_{ij})| \tag{4}$$

となるのであった (定理 9.2).

一方，判別式で考えると

$$\begin{aligned} d(\alpha_1, \cdots, \alpha_n) &= (\det(\alpha_i^{(j)}))^2 \\ &= (\det \sum_{k=1}^{n} a_{ik}\omega_k^{(j)})^2 \\ &= (\det(a_{ij}) \cdot \det(\omega_i^{(j)}))^2 \\ &= (N_K\mathfrak{A})^2 \cdot d(\omega_1, \cdots, \omega_n) \quad (\because (4)) \end{aligned}$$

を得る．この結果も重要だから番号を付しておこう (D_K は K の判別式).

$$d(\alpha_1, \cdots, \alpha_n) = (N_K\mathfrak{A})^2 \cdot D_K \tag{5}$$

さて $\mathfrak{A} = (\alpha) = \alpha\mathbb{O}_K$ の場合を考えてみよう．

$$\begin{aligned} d(\alpha\omega_1, \cdots, \alpha\omega_n) &= (\det(\alpha^{(j)}\omega_i^{(j)}))^2 \\ &= \left(\prod_{j=1}^{n} \alpha^{(j)}\right)^2 \cdot D_K \end{aligned}$$

ところで $(\alpha) = \alpha\mathbb{O}_K = [\alpha\omega_1, \cdots, \alpha\omega_n]$ だから (5) とあわせると次を得る：

$$(N_K(\alpha))^2 = \left(\prod_{j=1}^{n} \alpha^{(j)}\right)^2$$

そこで次の定義をおく：

定義　$\alpha \in \mathbb{O}_K$ に対して

$$N_K\alpha = \prod_{j=1}^{n} \alpha^{(j)} \quad (\text{共役積})$$

と定義し，これを α の (**絶対**) **ノルム**とよぶ.

すると上に示したことによって次を得る：

定理 11.7　$N_K(\alpha) = |N_K\alpha|$.

すなわち，単項イデアル (α) のノルムは数 α のノルムの絶対値である．

この結果を使ってイデアル類群の有限性を証明しよう．

補題　K の任意のイデアル $\mathfrak{A}$ は

$$|N_K\alpha| \leqq CN_K\mathfrak{A}$$

を満たす $\alpha(\neq 0)$ を含む．ここに C はある (代数体 K によって定まる) 定数である．

証明　$\omega_1, \cdots, \omega_n$ $(n = [K:\mathbb{Q}])$ を K の整数基とする．整係数の 1 次形式

$$x_1\omega_1 + \cdots + x_n\omega_n \tag{6}$$

に，$0 \leqq x_i \leqq g$ なる値を入れると，(6) から $(g+1)^n$ 個の数が得られる．ここに $g = [\sqrt[n]{N_K\mathfrak{A}}\,]$($\sqrt[n]{N_K\mathfrak{A}}$ を超えない最大整数) である．$(g+1)^n > N_K\mathfrak{A}$ なので，それらの数の中には $\bmod \mathfrak{A}$ で同一の剰余類に属するものが少くとも二つある (ディリクレの部屋割論法)．その差を取れば，

$$\alpha = \sum_{i=1}^{n} a_i\omega_i \neq 0 \quad (a_i \in \mathbb{Z}, |a_i| \leqq g)$$

なる元 $\alpha \in \mathfrak{A}$ の存在が保証されたことになる．(j)　$(j = 1, \cdots, n)$ を K の共役写像として，$M = n\max_{i,j}|\omega_i^{(j)}|$ と置くとき

$$|\alpha^{(j)}| = |\sum_i a_i\omega^{(j)}| \leqq gM \quad (j = 1, \cdots, n)$$

したがって

$$|N_K\alpha| = |\prod_{j=1}^{n} \alpha^{(j)}| \leqq (gM)^n$$

$C = M^n$ とすれば $g^n \leqq N_K\mathfrak{A}$ だから補題が証明された．∥

証明　(**定理** 11.6 **の証明**)　$c \in C_K$ とする．$c^{-1} \ni \mathfrak{A}$ なるイデアル $\mathfrak{A}$ を取る．補題によって

$$|N_K\alpha| \leqq CN_K\mathfrak{A}$$

を満たす $\alpha(\neq 0) \in \mathfrak{A}$ が取れる．$(\alpha) = \mathfrak{A}\mathfrak{B}$ と分解すれば $\mathfrak{B} \in c$ である．

$$|N_K\alpha| = N_K\mathfrak{A} \cdot N_K\mathfrak{B} \leqq CN_K\mathfrak{A}$$

$$\therefore \quad N_K\mathfrak{B} \leqq C \tag{7}$$

すなわち各 $c \in C_K$ は (7) を満たすような代表元 $\mathfrak{B}$ を含む．しかるに，この不等式を満たすようなイデアルは明らかに有限個であるから $|C_K| < +\infty$ が示された．∥

§ 4. 2 次体のイデアル類群と 2 次形式類群の対応

$h_K = 1$ ということは K には単項イデアルしか存在しない (つまり，$\mathbb{O}_K$ が単項イデアル整域をなす) ことである．したがってたとえば $h_{\mathbb{Q}} = 1$ である．また $K = \mathbb{Q}(\sqrt{-1})$ あるいは $K = \mathbb{Q}(\sqrt{-3})$ と置くと $h_K = 1$ であることも以前に証明した．円分体も p を $p \leqq 19$ なる素数とすれば円の p 分体の類数は 1 であることがわかっている．$p > 19$ なら類数は 1 ではない．

虚 2 次体 $\mathbb{Q}(\sqrt{-m})$ の類数が 1 となるのは

$$m = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

の 9 個しかなく，また実 2 次体 $\mathbb{Q}(\sqrt{m})$ の類数は無数の m に対して 1 であろうとガウスが予想したという．虚 2 次体の方の予想は 1966 年ベーカーによって肯定的に証明されたが，実 2 次体の方の予想は実例からいうと当然成り立つように見えてもまだ証明されていない．手近かに転がっているフィールズ賞を授賞されるであろう問題として推奨しておこう．他にも $n^2 + 1$ という形の素数は無数にあるという予想も，2 が $\bmod p$ の原始根となるというような素数 p は無数にあるという予想も，いずれも解決されれば歴史に名を残すことは請け合いである．これらの難問は直接的に証明を試みるよりは何かの理論の副産物として解決される可能性の方が高いだろうと思われる．

なお，ガウスが類数に関する予想を立てたということは，ガウスは 2 次体のイデアル論を知っていたのかという早とちりをする人もいるかもしれない．実は 2 次形式の合成理論 (その中で一番簡単なのはブラフマグプタの恒等式であり，次に簡単なのはこれを一般化した

$$(x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2) = (x_1x_2 + Dy_1y_2)^2 + D(x_1y_2 - x_2y_1)^2$$

であるが) はオイラー，ラグランジュ等を経てガウスによって徹底的に研究された (ガウス [5])．2 元 2 次形式 $aX^2 + bXY + cY^2$ の合成は 2 次体のイデアルの積に対応し，イデアル類群と 2 次形式のある同値関係による剰余類群が同型になるのである．

これについては日本語では河田 [11] に解説が見られるが，本書でもサワリの部分を紹介しておこう．

$$SL_2(\mathbb{Z})^{\pm} = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \middle| ru - st = \pm 1 \right\}$$

とする．$SL_2(\mathbb{Z})^{\pm}$ は第 1 章で登場した群である．本節では 2 元 2 次形式

$$f(X,Y) = aX^2 + bXY + cY^2$$

はつねに $a,b,c \in \mathbb{Z}$ であるとする．$f(X,Y)$ は

$$f(X,Y) = (X,Y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$$

と行列を使って表せる．

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} X' \\ Y' \end{pmatrix}, \quad \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})^{\pm}$$

という変数変換を施せば，新たに

$$\begin{aligned} f'(X',Y') &= (X',Y')\begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} X' \\ Y' \end{pmatrix} \\ &= (X',Y')\begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix}\begin{pmatrix} X' \\ Y' \end{pmatrix} \end{aligned}$$

ただし

$$\begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

という 2 元 2 次形式 f' を得る．f と f' とが同じ整数を表現できること，すなわち $m \in \mathbb{Z}$ に対して

$$\exists X,Y(\in \mathbb{Z}); f(X,Y) = m \Longleftrightarrow \exists X,Y(\in \mathbb{Z}); f'(X,Y) = m$$

が成り立つことは変換行列が $SL_2(\mathbb{Z})^{\pm}$ の元であることによって明らかであるから，次のように定義するのも当然だろう．

定義　2 次形式 f がもう一つの 2 次形式 g に上のような変数変換によって移り得るとき f は g に**対等**であるといって

$$f \sim g$$

と表す．

$\sim$ が 2 元 2 次形式間の同値関係であることは $SL_2(\mathbb{Z})^{\pm}$ が群をなすことから明らかである．

問題　2 元 2 次形式 $f(X,Y) = aX^2 + bXY + cY^2$ の**判別式** D を $D = b^2 - 4ac$ によって定義するとき $f \sim g$ ならば，f, g の判別式は一致することを示せ．

さて 2 元 2 次形式と 2 次体のイデアルの対応を与えよう．2 次体 $K = \mathbb{Q}(\sqrt{m})$ $(m \in \mathbb{Z};$ 平方因子を含まない$)$ の判別式を D_K とする．K のイデアル $\mathfrak{A}$ は $\mathbb{Z}$ 上階数 2 の自由加群だから

$$\mathfrak{A} = [\alpha_1, \alpha_2] = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 \quad (\alpha_1, \alpha_2 \in \mathbb{O}_K)$$

と表せる．$\mathfrak{A}$ に対して 2 元 2 次形式

$$\begin{aligned} AX^2 + BXY + CY^2 &= N_K(\alpha_1 X + \alpha_2 Y) \\ &= (\alpha_1^{(1)} X + \alpha_2^{(1)} Y)(\alpha_1^{(2)} X + \alpha_2^{(2)} Y) \end{aligned}$$

を考える．このとき次が成り立つ：

命題

1. $A, B, C \in \mathbb{Z}$
2. $B^2 - 4AC = (N_K\mathfrak{A})^2 D_K$
3. $(A, B, C) = N_K\mathfrak{A}$

証明　$A = \alpha_1^{(1)}\alpha_1^{(2)} = N_K\alpha_1$，$B = \alpha_1^{(1)}\alpha_2^{(2)} + \alpha_2^{(1)}\alpha_1^{(2)} = T_K(\alpha_1^{(1)}\alpha_2^{(2)})$，$C = \alpha_2^{(1)}\alpha_2^{(2)} = N_K\alpha_2$，ここに $T_K(\theta) = \theta^{(1)} + \theta^{(2)}$ とする．$T_K(\theta) \in \mathbb{Q}$ と

$\theta \in \mathbb{O}_K$ ならば $T_K(\theta) \in \mathbb{Z}$ は明らかである．故に 1. が成り立つ．

2.　$B^2 - 4AC = (\alpha_1^{(1)}\alpha_2^{(2)} - \alpha_1^{(2)}\alpha_2^{(1)})^2 = d(\alpha_1, \alpha_2) = D_K(N_K\mathfrak{A})^2$(p.167 式 (5) 参照).

3.　$\alpha_i \in \mathfrak{A}\quad (i = 1, 2)\quad \therefore\ \mathfrak{A}|(\alpha_i)\quad \therefore\ N_K\mathfrak{A}|N_K(\alpha_i)$. 一方，$N_K(\alpha_i) = \pm N_K\alpha_i$ だから $N_K\mathfrak{A}|A, N_K\mathfrak{A}|C$ がわかる．2. より

$$\begin{aligned} B^2 &\equiv 4AC \pmod{(N_K\mathfrak{A})^2} \\ &\equiv 0 \pmod{(N_K\mathfrak{A})^2} \end{aligned}$$

故に $N_K\mathfrak{A}|B$. そこで

$$A = aN_K\mathfrak{A}, \quad B = bN_K\mathfrak{A}, \quad C = cN_K\mathfrak{A}$$

と置くと $b^2 - 4ac = D_K$ となる．$D_K = m$, または $4m$ であるから，$d = (a, b, c)$ の素因数は 2 以外にありえない．$2|d$ とすると $m \equiv 2$, または $\equiv 3 \pmod 4$ の場合である．しかしこれは

$$\begin{aligned} m = \frac{D_K}{4} &= \left(\frac{b}{2}\right)^2 - 4 \cdot \frac{a}{2} \cdot \frac{c}{2} \\ &\equiv 0, 1 \pmod 4 \end{aligned}$$

に矛盾する．故に $d = 1$ である． ‖

したがって

$$AX^2 + BXY + CY^2 = (aX^2 + bXY + cY^2)N_K\mathfrak{A}$$

と置けて，$b^2 - 4ac = D_K$ を満たす．要約すれば，整係数 2 元 2 次形式

$$\frac{N_K(\alpha_1 X + \alpha_2 Y)}{N_K\mathfrak{A}}$$

は判別式 D_K を持ち，原始的である．これでイデアル類と 2 元 2 次形式の類との対応はほぼ想像がつくと思う．

2 次形式の類数の有限性はラグランジュによって証明され，最後にガウスが 2 次形式の合成という概念を導入して 2 次形式の類に群構造を与えたのだった．

今 $\mathfrak{A} = [\alpha_1, \alpha_2], \mathfrak{B} = [\beta_1, \beta_2]$ を K のイデアルとし，$\mathfrak{C} = \mathfrak{A}\mathfrak{B} = [\gamma_1, \gamma_2]$ とすると

$$\alpha_i\beta_j = \sum_{k=1}^{2} c_{ijk}\gamma_k, \quad c_{ijk} \in \mathbb{Z} \ \ (i,j=1,2)$$

と表せる.

$$f(X_1,X_2) = \frac{N_K(\alpha_1X_1+\alpha_2X_2)}{N_K\mathfrak{A}}, \qquad g(Y_1,Y_2) = \frac{N_K(\beta_1Y_1+\beta_2Y_2)}{N_K\mathfrak{B}}$$

を $\mathfrak{A}, \mathfrak{B}$ に対応する 2 次形式としよう. このとき

$$\begin{aligned}(\alpha_1X_1+\alpha_2X_2)(\beta_1Y_1+\beta_2Y_2) &= \sum_{i=1}^{2}\sum_{j=1}^{2}\alpha_i\beta_jX_iY_j \\ &= \sum_{i,j}\sum_{k} c_{ijk}\gamma_kX_iY_j \\ &= \sum_{k=1}^{2}\gamma_k\left(\sum_{i,j=1}^{2} c_{ijk}X_iY_j\right)\end{aligned}$$

そこで

$$Z_k = \sum_{i,j=1}^{2} c_{ijk}X_iY_j \quad (k=1,2)$$

と置けば,

$$\begin{aligned}f(X_1,X_2)g(Y_1,Y_2) &= \frac{N_K(\alpha_1X_1+\alpha_2X_2)}{N_K\mathfrak{A}}\cdot\frac{N_K(\beta_1Y_1+\beta_2Y_2)}{N_K\mathfrak{B}} \\ &= \frac{N_K(\alpha_1X_1+\alpha_2X_2)(\beta_1Y_1+\beta_2Y_2)}{N_K\mathfrak{C}} \\ &= \frac{N_K(\gamma_1Z_1+\gamma_2Z_2)}{N_K\mathfrak{C}}\end{aligned}$$

を得る. これを $h(Z_1,Z_2)$ とする. とくに, $\mathfrak{A}=(\alpha)$ という場合を考えてみれば, $\mathfrak{A}\mathfrak{B}=\alpha\mathfrak{B}=[\alpha\beta_1,\alpha\beta_2]$ となって$h=g$を得る. さらに基底$\{\alpha_1,\alpha_2\}$, $\{\beta_1,\beta_2\}$ の取り方は一意ではないことを考慮すれば, f の類と g の類から合成 h の類が一意に定まる, という形になる. これによって, もう少し精緻な考察を要するが, 次のようなタイプの命題が証明される：

命題　2 次体 $\mathbb{Q}(\sqrt{D})$ のイデアル類群は判別式が D の 2 元 2 次形式の類のなす群と同型である.

この命題がラグランジュ, ガウスの業績と現代の 2 次体論を結ぶ糸である. 言い換えれば, 2 次体論の持つ歴史的背景の説明である.

最後に，2 元 2 次形式 $f(x,y)$ がどういう素数 p を表し得るか，つまり

$$f(x,y)=p$$

に解があるか否かについて一般的な解答を与えておこう．

定理 11.8　2 次体 $K=\mathbb{Q}(\sqrt{m})$ の判別式を D とする．素数 p が判別式 D のある原始 2 元 2 次形式で表現される条件は (p) が K において素イデアルではないことである．

証明 (証明には定理 11.10 を使う)　まず $(p)=\mathfrak{p}_1\mathfrak{p}_2, N_K\mathfrak{p}_i=p$ の場合を扱う ($\mathfrak{p}_1=\mathfrak{p}_2$ の場合も含める)．$\mathfrak{p}_1=[\pi_1,\pi_2]$ とする (つまり，π_1,π_2 は $\mathfrak{p}_1$ の基である)．対応する原始 2 元 2 次形式を $f(X,Y)$ とする：

$$f(X,Y)=\frac{N_K(\pi_1X+\pi_2Y)}{N_K\mathfrak{p}_1}$$

$p\in\mathfrak{p}_1$ だから $p=\pi_1X_0+\pi_2Y_0\ \ (X_0,Y_0\in\mathbb{Z})$ と表せる．共役を取って，$p=\overline{\pi_1}X_0+\overline{\pi_2}Y_0$ である．$\therefore\ f(X_0,Y_0)=\dfrac{p^2}{p}=p$

次に (p) が K でも素イデアルである場合，したがって，$N_K(p)=p^2$ の場合を考えよう．仮りに判別式 D の原始 2 元 2 次形式 $f(X,Y)$ によって $p=f(X_0,Y_0)$ と表せたとしよう．先述の対応によってイデアル $\mathfrak{A}=[\alpha_1,\alpha_2]$ と表せ，

$$f(X,Y)=\frac{N_K(\alpha_1X+\alpha_2Y)}{N_K\mathfrak{A}}$$

となる．$f(X_0,Y_0)=p$ だから上式から

$$p\cdot N_K\mathfrak{A}=N_K(\alpha_1X_0+\alpha_2Y_0)$$

$\mathfrak{A}$ の p 成分を $(p)^m$ とすれば $N_K(p)=p^2$ によって左辺の p 成分は p^{2m+1} である．$\alpha_1X_0+\alpha_2Y_0$ の p 成分を $(p)^n$ とすれば $\overline{\alpha_1}X_0+\overline{\alpha_2}Y_0$ の p 成分も $(p)^n$ だから右辺は p^{2n} でちょうど割り切れる．これは矛盾である．すなわち $p=f(X_0,Y_0)$ と表せることはない． ∥

本定理と p の 2 次体における分解を決定する定理 (定理 11.10) とを組み合わせれば，フェルマー，オイラー以来の研究はここに完結を見たことになる．

最後に類数の有限性についての歴史に関して一言．2 次体の場合は 2 元 2 次の形式類の言葉でラグランジュによって示されたことは先述．円分体の場合はクンマーによって示された．その論文の中で，高次の形式類の有限性という形でディリクレが証明したと聞いているが発表されないので云々と書いている．一般の代数体の場合の証明はデデキントが最初であろう．

§5. 有理素数の代数体における素イデアル分解

K を n 次代数体とする．p を素数とし $(p) = p\mathbb{O}_K$ とすると，(p) は K では素イデアルとは限らない．このことは既に $K = \mathbb{Q}(\sqrt{-1}\,)$ の場合にも起こったことであった．(p) が K においてどのように素イデアル分解されるかを一般的に考察してみよう．

まず K において

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \quad (e_i > 0)$$

と相異なる素イデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ の冪積に分解されたとする．$(p) \subsetneqq \mathfrak{p}_i$ だから $p \in \mathfrak{p}_i$ である．故に $\mathfrak{p}_i \cap \mathbb{Z} = (p)(= p\mathbb{Z})$ であるから

$$N_K\mathfrak{p}_i = p^{f_i} \quad (i = 1, \cdots, g)$$

と表せる．定理 11.5 を適用すると

$$N_K(p) = (N_K\mathfrak{p}_1)^{e_1} \cdots (N_K\mathfrak{p}_g)^{e_g} = p^{e_1 f_1} \cdots p^{e_g f_g}$$

が得られる．$N_K(p) = (\mathbb{O}_K : p\mathbb{O}_K) = p^n$ だから左辺は p^n である．故に

$$e_1 f_1 + \cdots + e_g f_g = n \tag{8}$$

という重要な等式が得られる．

$K = \mathbb{Q}(\sqrt{-1}\,)$ の場合に戻って考えてみよう．

1. $p = 2$ ならば $(2) = (\lambda)^2$
2. $p \equiv 1 \pmod 4$ ならば $(p) = (\pi_1)(\pi_2)$, $(\pi_1) \neq (\pi_2)$

3. $p \equiv -1 \pmod 4$ ならば (p) は素イデアルのまま

という結論であった (定理 5.5 の系) が,

1. の場合,　$e=2,\ f=1,\ g=1$

2. の場合,　$e=1,\ f=1,\ g=2$

3. の場合,　$e=1,\ f=2,\ g=1$

というパターンであることがわかる.

e_i を $\mathfrak{p}_i$ の**分岐指数**, f_i を $\mathfrak{p}_i$ の**次数**という. $e_i>1$ のとき $\mathfrak{p}_i$ は $K/\mathbb{Q}$ で**分岐**すると言い, $e_i=1$ のとき $\mathfrak{p}_i$ は $K/\mathbb{Q}$ で**不分岐**であると言い慣わしている. 時には, $e_i>1$ なる i があるとき (p) が分岐するとも言う. $\mathbb{Q}(\sqrt{-1})$ の場合では, (2) だけが分岐している. (これは定理 11.10 に見るように $\mathbb{Q}(\sqrt{-1})$ の判別式が $4\ (=2^2)$ であるという事実に基づく.)　$\mathbb{Q}(\sqrt{-1})$ においての分解の様子が mod 4 という $\mathbb{Z}$ の世界の言葉だけで記述されていることに注目すべきで, 円分体論, その一般化である類体論はすべて同じパターンのくり返しである. 言い換えれば, 代数的整数論というのは拡大体における素イデアルの分解の様子を基礎体でのデータで記述することを主要な目標の一つとする学問であると言うことができる.

§ 6.　素イデアル分解の具体的な求め方

$K=\mathbb{Q}(i)$ において, 素数 p がどのように分解するかは X^2+1 が mod p でどのように分解するかで決まることを第 5 章 §3 で述べたが, この考察は次のように一般化することができる：

定理 11.9　K を n 次代数体, $\mathbb{O}_K$ を K の整数環とし, $\mathbb{O}_K=\mathbb{Z}[\omega]$ を満たす $\omega \in \mathbb{O}_K$ が存在すると仮定する. (すなわち, 整数基として $1,\omega,\omega^2,\cdots,\omega^{n-1}$ が取れるとする.) また, $f(X)$ を ω の満たすモニック既約多項式とする. p を素数として, mod p で

$$f(X) \equiv p_1(X)^{e_1}\cdots p_g(X)^{e_g} \pmod p$$

(ここに $p_i(X) \in \mathbb{Z}[X]$ はモニック, 次数 f_i, さらに mod p で既約かつ互い

に素とする) と因数分解されれば，(p) は K において

$$(p)=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g},\quad N_K\mathfrak{p}_i=p^{f_i}$$

という形に素イデアル分解される．ここに各 $\mathfrak{p}_i$ は

$$\mathfrak{p}_i=(p_i(\omega),p)$$

である．

補題　F を体とし，$f(X),g(X),h(X)\in F[X]$ はモニックであるとする．対応

$$\varphi(X)\bmod h(X)\rightsquigarrow(\varphi(X)\bmod f(X),\ \varphi(X)\bmod g(X))$$

によって $F[X]/(h(X))\simeq F[X]/(f(X))\oplus F[X]/(g(X))$ となるならば，

$$h(X)=f(X)\cdot g(X),\quad (f,g)=1$$

が成り立つ．

証明　まず写像が well defined であることによって $f|h,\ g|h$ を得る．次に $(0\bmod f,\ 1\bmod g)$ の原像が存在するはずだから

$$\varphi\equiv 0\pmod f,\quad \varphi\equiv 1\pmod g$$

なる $\varphi(X)\in F[X]$ が取れる．故に $\varphi=ff',\varphi=1+gg'$ と書けるから $ff'-gg'=1$ となって，$(f,g)=1$ がわかる．このとき $F[X]/(f)\oplus F[X]/(g)\simeq F[X]/(fg)$ だから $(fg)=(h)$ が結論できる．モニック性は $fg=h$ を保証する．‖

証明 (定理 11.9 の証明)

$$(p)=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g},\quad \mathfrak{p}_i\neq\mathfrak{p}_j\ (i\neq j),\quad e_i>0$$

を (p) の K における素イデアル分解とする．このとき孫子の定理によって

$$\mathbb{Z}[\omega]/(p)\simeq\mathbb{Z}[\omega]/\mathfrak{p}_1^{e_1}\oplus\cdots\oplus\mathbb{Z}[\omega]/\mathfrak{p}_g^{e_g}$$

が成り立つ．

$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ とする．$f(X)\in\mathbb{Z}[X]$ を ω の満たすモニックな既約多項式とすると，

$$\mathbb{F}_p[X]/(\overline{f}) \simeq \mathbb{Z}[\omega]/(p)$$

が成り立つ．(ここに $\overline{f} = f(X) \bmod p$, $(\overline{f}) = \overline{f} \cdot \mathbb{F}_p[X]$ である.) 実際, $\mathbb{Z}[X]/(f) \simeq \mathbb{Z}[\omega]$ であるから $\mathbb{Z}[\omega]$ のイデアル (p) に対しては $(p, f)/(f)$ なるイデアルが対応している．故に

$$\begin{aligned}\mathbb{Z}[\omega]/(p) &\simeq (\mathbb{Z}[X]/(f))/((p,f)/(f)) \\ &\simeq \mathbb{Z}[X]/(p,f) \\ &\simeq (\mathbb{Z}[X]/(p))/((p,f)/(p)) \\ &\simeq \mathbb{F}_p[X]/(\overline{f})\end{aligned}$$

だからである．次に

$$\mathbb{Z}[\omega]/\mathfrak{p}_i \simeq \mathbb{F}_p[X]/(\overline{p_i})$$

なる mod p でのモニック既約多項式 $p_i(X) \in \mathbb{Z}[X]$ を取る ($p_i(X)$ の次数は $N_K\mathfrak{p}_i$ の定義によって f_i 次である)．$p_i(X)$ の取り方によって $p_i(\omega) \equiv 0 \pmod{\mathfrak{p}_i}$ である．そして $p_i(\omega) \not\equiv 0 \pmod{\mathfrak{p}_i^2}$ でもある．仮りに $p_i(\omega) \equiv 0 \pmod{\mathfrak{p}_i^2}$ なら $\mathbb{Z}[\omega]/\mathfrak{p}_i \simeq \mathbb{Z}[\omega]/\mathfrak{p}_i^2$ なる矛盾を生じるからである．明らかに

$$\mathbb{Z}[\omega]/\mathfrak{p}_i^{e_i} \simeq \mathbb{F}_p[X]/(\overline{p_i}^{e_i})$$

であるから，以上を総合して

$$\mathbb{F}_p[X]/(\overline{f}) \simeq \mathbb{F}_p[X]/(\overline{p_1}^{e_1}) \oplus \cdots \oplus \mathbb{F}_p[X]/(\overline{p_g}^{e_g})$$

を得る．補題によって

$$f(X) \equiv p_1(X)^{e_1} \cdots p_g(X)^{e_g} \pmod{p}$$

かつ

$$(p_i, p_j) = 1 \quad (i \neq j)$$

が成り立つ．ここで $f(X) \bmod p$ の因数分解は $\mathbb{F}_p[X]$ が U.F.D. なので一意的であることに注意する．また，$p_i(X)$ の定義の仕方によって $p_i(\omega) \equiv 0 \pmod{\mathfrak{p}_i}$, $\not\equiv 0 \pmod{\mathfrak{p}_i^2}$ が成り立つ．$(p_i, p_j) = 1$ $(i \neq j)$ だから $p_j(\omega) \not\equiv 0 \pmod{\mathfrak{p}_\mathrm{i}}$ である．すなわち $p_i(\omega) \not\equiv 0 \pmod{\mathfrak{p}_\mathrm{j}}$ $(i \neq j)$ である．故に

$$\mathfrak{p}_i = (p, p_i(\omega)) \quad (i = 1, \cdots, g)$$

である．∥

定理 11.9 は $\mathbb{O}_K = \mathbb{Z}[\omega]$ の場合しか適用できないが，2 次体ばかりではなく円分体もこの条件を満たすので適用範囲は広い．

定理 11.9 を 2 次体に適用すると次のような結果を得る．平方剰余という概念がどうして発生したのか，その起源はわからないにしても，実に重要な役割を果たすことが徐々に明らかになってきたことはわかるだろう．

$K = \mathbb{Q}(\sqrt{m})$，m は平方因子を含まない整数，とするとき判別式 D_K は

$$D_K = \begin{cases} m & (m \equiv 1 \pmod 4) \\ 4m & (m \not\equiv 1 \pmod 4) \end{cases}$$

となることを思い出しておかねばならない (定理 9.6 参照).

定理 11.10　m を平方因子を含まない整数とし，$K = \mathbb{Q}(\sqrt{m})$ とする．素数 p から生成される K のイデアル $(p) = \{px \mid x \in \mathbb{O}_K\}$ の K における素イデアル分解は次の通りである：

1. $p|D_K$ のとき，かつそのときに限り (p) は分岐で

$$(p) = \mathfrak{p}^2, \quad N_K\mathfrak{p} = p$$

2. $p \nmid D_K$ とする．$p \neq 2$ の場合は，

$$\left(\frac{m}{p}\right) = 1 \text{ ならば } (p) = \mathfrak{p}_1\mathfrak{p}_2,\ N_K\mathfrak{p}_1 = N_K\mathfrak{p}_2 = p$$

$$\left(\frac{m}{p}\right) = -1 \text{ ならば } (p) = \mathfrak{p},\ N_K\mathfrak{p} = p^2$$

$p = 2$ の場合は，(これは $m \equiv 1 \pmod 4$ の場合に限るのであるが)

$$m \equiv 1 \pmod 8 \quad \text{ならば} \quad (2) = \mathfrak{p}_1\mathfrak{p}_2,\ N_K\mathfrak{p}_1 = N_K\mathfrak{p}_2 = 2,$$

$$m \equiv 5 \pmod 8 \quad \text{ならば} \quad (2) = \mathfrak{p},\ N_K\mathfrak{p} = 2^2.$$

問題　定理 11.10 を証明せよ．

以上において $N_K\mathfrak{p}$ は $\mathfrak{p}$ のノルム，すなわち剰余体 $\mathbb{O}_K/\mathfrak{p}$ の元の総数を表す．また $\mathfrak{p}_1 \neq \mathfrak{p}_2$ とする．$(p) = \mathfrak{p}$ とは (p) がそのままで K の素イデアル

であることを示している．

定理 11.10 から，$K/\mathbb{Q}$ で分岐する素イデアル (あるいは，その下にある素数) は判別式 D_K の約因子になっているものしかないのではないかと予想されるが，実際それは正しい：

定理 11.11 (判別定理)　素数 p が $K/\mathbb{Q}$ で分岐するための条件は p が判別式 D_K の約数であることである．

証明 ($\mathbb{O}_K = \mathbb{Z}[\omega]$ となる ω の存在する場合だけを扱う．)　K において

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

と素イデアル分解されるとする．$\mathfrak{p}_1 = \mathfrak{p}, e_1 = e$ とし，$\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g} = \mathfrak{A}$ と記そう．そうすると

$$(p) = \mathfrak{p}^e \mathfrak{A}, \quad (\mathfrak{p}, \mathfrak{A}) = 1$$

である．定理 11.10 の証明と同じ記号で

$$f(X) \equiv p(X)^e A(X) \pmod{p}$$

とする．両辺の形式的導関数を作ると

$$f'(X) \equiv ep(X)^{e-1} p'(X) A(X) + p(X)^e A'(X) \pmod{p}$$

ω を代入すると

$$f'(\omega) \equiv ep(\omega)^{e-1} p'(\omega) A(\omega) + p(\omega)^e A'(\omega) \pmod{p}.$$

$p(\omega)^e \equiv 0 \pmod{\mathfrak{p}^e}$ である．また ω が $\bmod\ \mathfrak{p}$ で満たす既約多項式が $p(X)$ だから $p'(\omega) \not\equiv 0 \pmod{\mathfrak{p}}$．最後に，$A(\omega) \not\equiv 0 \pmod{\mathfrak{p}}$ だったから

$$f'(\omega) \equiv ep(\omega)^{e-1} p'(\omega) A(\omega) \pmod{\mathfrak{p}^e}$$

より

$$f'(\omega) \equiv 0 \pmod{\mathfrak{p}} \iff e > 1$$

を得る．一方，$f(X) = (X - \omega^{(1)})(X - \omega^{(2)}) \cdots (X - \omega^{(n)})$(ただし，$\omega^{(1)} = \omega$) だから $f'(\omega) = (\omega - \omega^{(2)}) \cdots (\omega - \omega^{(n)})$ を得る．$f'(\omega) \in K$ であるから $N_K f'(\omega)$ は意味を持つが，さらに共役写像を $K/\mathbb{Q}$ を含むガロア拡大 $L/\mathbb{Q}$ に延長して考えておくことによって，

$$
\begin{aligned}
N_K f'(\omega) &= \prod_{i=1}^{n} f'(\omega)^{(i)} \\
&= \prod_{i \neq j} (\omega^{(i)} - \omega^{(j)}) \\
&= (-1)^{\frac{n(n-1)}{2}} D_K
\end{aligned}
$$

となる．故に $\mathfrak{p}$ が分岐する条件は $\mathfrak{p} | f'(\omega)$ となり，このときは $p | D_K$ を得る．逆に $p | D_K$ ならば $\mathfrak{p} | f'(\omega)^{(i)}$ なる i が存在する．これより，$K/\mathbb{Q}$ を含むガロア拡大 $L/\mathbb{Q}$ を考えればわかるように，$\mathfrak{p}_k | f'(\omega)$ を満たす k $(k = 1, \cdots, g)$ が存在するはずである．上の考察で $\mathfrak{p}_k$ を $\mathfrak{p}$ として考えれば，$\mathfrak{p}_k$ が分岐することになる．なお以上の考察には次章の知識 (p.191 の命題) を使った． ‖

第12章　ガロアの理論

§ 1. 代数的閉包

これまで体としては，代数体，すなわち有理数体の有限次拡大体を主たる対象としてきた．しかし今後は代数体の素イデアルによる剰余体が大きな役割を果たすことになるので，良い機会だから，一般的な体について基礎事項でありながら，代数体では考える必要がなかった事項，とりわけ標数という概念と代数的閉包の存在について本節でまとめて考察しておこう．

K を体とし，その乗法単位元を 1_K と記す．慣れてくると，1_K をずぼらに 1 と書いても勘違いする可能性はなくなるが，とりあえず最初のうちは節度を守って 1_K と記すことにする．

1_K を n 個加えた $\overbrace{1_K + \cdots + 1_K}^{n}$ を $n \cdot 1_K$ と記す．厳密に言えば，回帰的 (recursive) に

$$1 \cdot 1_K = 1_K, \quad (n+1) \cdot 1_K = n \cdot 1_K + 1_K$$

と定義するのである．(ここに 1 とか n とかは体 K の元ではなく，普通の自然数である．$\mathbb{N}$ がスカラーとして K に左から作用していると考えればよい．) また $n < 0$ のときは $n \cdot 1_K = -((-n) \cdot 1_K)$．$n = 0$ に対しては $0 \cdot 1_K = 0_K$(K の加法単位元) とする．

定義　$n \cdot 1_K = 0_K$ となるような自然数 n が存在するとき，そのような性

質を持つ最小の自然数を体 K の**標数** (characteristic) といって，$\mathrm{char}(K)$ と表す．任意の $n \in \mathbb{N}$ に対して $n \cdot 1_K \neq 0_K$ のときは，K の標数は 0 であるとする．

たとえば，p が素数のとき，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は標数 p を持つ．また代数体の標数は 0 である．

定理 12.1　体の標数は 0 か，あるいは素数である．

証明　$\varphi : \mathbb{Z} \longrightarrow K$ を $\varphi(n) = n \cdot 1_K$ によって定義する．φ は環準同型写像である．故に準同型定理から K は $\mathbb{Z}/A$ と同型な部分環を含む．ここに A は φ の核 $\{x(\in \mathbb{Z}) \mid \varphi(x) = 0_K\}$ である．$\mathbb{Z}$ のイデアル A は $A = (m)$ と書けるが，K は体だから零因子を含まないし，また 2 個以上の元を持つので m が合成数や ± 1 ということは起こり得ない．故に $m = p$(素数)，あるいは $m = 0$ である．∥

標数 p の場合 K には $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ と同型な体が含まれることになり，標数 0 の場合 K は $\mathbb{Q}$ と同型な体を含むことになる．真の部分体を持たないような体のことを**素体**ということにすると，素体は $\mathbb{Q}$ か $\mathbb{F}_p$ かに同型ということがわかったことになる．

次に代数的閉包の話をしよう．有理数体 $\mathbb{Q}$ の場合には $\overline{\mathbb{Q}}$ という都合のよい体 (複素数体の部分体) が存在して，ここではどんな多項式も 1 次式に因数分解される．しかし，たとえば $\mathbb{F}_p$ の場合はどうだろうか．ここでは $X^2 + 1 = 0$ という方程式は $p \equiv 1 \pmod 4$ なら解を持つが，そうでないなら解を持たない．このとき $i^2 + 1 = 0$ と同様の発想で $X^2 + 1 = 0$ の解が存在するというように出来ないだろうか．また $X^2 - 2 = 0$ はどうだろうか．

定理 12.2　K を体とし，$f \in K[X]$ を K 上既約な多項式とすると，

$$L = K(\theta),\quad f(\theta) = 0,\quad [L:K] = \deg f$$

なる K の拡大体 ($f(X)$ の**根体**と呼ばれる) が存在する.

証明　体 $K[X]/(f)$ を L とする. $a \rightsquigarrow a \bmod f$ なる単射によって K は L の中に埋蔵される. このようにして L は K と同型な体を部分体として含むので, それを K とみなすことにする. このとき $\theta = \overline{X} = X \bmod f$ とすれば

$$f(\theta) = f(\overline{X}) = \overline{f(X)} = \overline{0} = 0$$

が成り立つ. ここに, $\overline{f}$ は f と, 同一視されていることに注意. ∥

[注意]　K は L の中に埋蔵されているのであって, 本当に $K \subsetneqq L$ なのではない, ということが気になるなら, 記号 Θ を準備して K を部分集合として含む集合 $K(\Theta)$ を, $K[X]/(f(X))$ と同型になるように定義すればよい. しかし, こういうことも凝りだせば, 変数とは何かといったことを含め, 色々細部にこだわらなければならなくなるから, ここでは, そういったことは集合論の基本的な知識があれば, 完全に解決できるのだという保証をするに留めておきたい (詳細は, 足立 [21]pp.136–138 参照).

系　K を体とし, $f(X) \in K[X]$ とする. $f(X)$ がそこでは 1 次式に分解されるような K の拡大体が存在する. このような体を $f(X)$ の**分解体**と言い, 最小の分解体を**最小分解体**という.

証明　K 上の $f(X)$ の根体を K_1 とし, K_1 において $f(X)$ を因数分解する. そのとき 1 次ではない既約因子 $f_1(X)$ が存在すれば K_1 上 $f_1(X)$ の根体を作り K_2 とする. このように続ければ, $\deg f$ 以内の回数で, $f(X)$ が 1 次式に分解される拡大体 K' に到達する. $f(X)$ のどの分解体も K' と同型な部分体を含むことは明らかである. ∥

抽象代数学の威力をまざまざと示すテクニックではないだろうか. ガウスは n 次方程式には n 個の解があるという方程式論の基本定理の証明を学位論文

として提出したのだが，その中でオイラーを始めとする先人の証明は「代数方程式 $f(X)=0$ には解 α が存在するとして，その α が複素数であること，すなわち $\alpha=a+bi$ $(a,b\in\mathbb{R})$ と表せることを証明したにすぎない」と指摘した．鋭い指摘ではあるが，抽象代数学の普及した今となっては，根体の存在定理によって多項式の零点の存在は保証されることになり，オイラーたちの見過ごしも大したミスではなかったことになるのである．こうした数学史的事実をふまえると上の定理の意義はより鮮明なものとなるだろう．抽象的な体論を創始したのはシュタイニッツだが，彼の偉業を称える意味もこめて，ここに記しておきたい．

ところで方程式が出てくるたびにその根体を作っているのではまどろっこしい．あらゆる方程式が解を持つような，そう，$\mathbb{Q}$ に対する $\overline{\mathbb{Q}}$ のような体の存在を仮定できないものだろうか．もちろんこれは可能である．すぐ後で定義するようにこうした体を K の**代数的閉包**という．

以上のお話を定義・定理の形にまとめよう：

定義　体 Ω が**代数的に閉じている**とは，任意の $f(X)\in\Omega[X]$ が Ω において 1 次式に分解されることをいう．

例えば複素数体 $\mathbb{C}$ は代数的に閉じている．方程式論の基本定理は「複素数体は代数的に閉じている」とカッコ好く表現できるのである．

例題　$\mathbb{Q}$ 上代数的な数全体のなす体 $\overline{\mathbb{Q}}$ は代数的に閉じていることを示せ．

解答

$$f(X)=a_0+a_1X+\cdots+a_nX^n\in\overline{\mathbb{Q}}[X]$$

とせよ．方程式論の基本定理から $f(\theta)=0$ なる $\theta\in\mathbb{C}$ が存在することが判る．$K=\mathbb{Q}(a_0,\cdots a_n)$, $L=K(\theta)$ とすれば $[L:\mathbb{Q}]=[L:K][K:\mathbb{Q}]<\infty$ であるから，θ は $\mathbb{Q}$ 上有限次の方程式の根である．$(1,\theta,\theta^2,\cdots$ を考えると

よい.）故に $\theta \in \overline{\mathbb{Q}}$ である.

$\mathbb{C}$ のかわりに $\overline{\mathbb{Q}}$ を好んで使うのは，$\mathbb{C}$ には超越数，つまり代数方程式の根とならない数 (たとえば，e や π など) が含まれているからである．代数学としては有理数体上代数的であるような数だけを集めた体 $\overline{\mathbb{Q}}$ を作業の場としたいのである.

定義　K を体とする．Ω/K が次の条件を満たすとき，Ω は K の代数的閉包であると呼ばれる：

1. Ω は代数的に閉じている.
2. Ω/K は代数拡大である．すなわち $\forall\alpha \in \Omega$ は K 上の代数方程式の根となる．(これを α は K 上代数的であるという.)

$\mathbb{C}$ は $\mathbb{Q}$ の代数的閉包ではない．$\pi \in \mathbb{C}$ など，$\mathbb{Q}$ 上代数的でない元が存在するからである．$\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数的閉包である.

定理 12.3 (シュタイニツの定理)　K を体とすると，K の代数的閉包が存在し，K 上の同型を除いて唯一である.

存在証明はいく通りか考えられるが，いずれも整列原理，あるいはツォルンの補題という，選択公理と同値な命題を必要とする．次に挙げるのはシュタイニツの元の証明に基づく．要するに基礎体 K のすべての多項式の最小分解体を次々に作って積み重ねていけば，その全体が K の代数的閉包 $\overline{K}$ になるだろう，それを厳密に証明しようというのである．一意性については次節に述べる.

補題　Ω/K を代数拡大とする．Ω が代数的に閉じているためには，Ω がすべての K 係数多項式の分解体となっていることが必要十分である.

証明　$f(X)$ を Ω 上既約な多項式とする．定理 12.2 によって $f(X)=0$ の根 α を Ω に添加して Ω' とすることができる：$\Omega' \simeq \Omega[X]/(f)$．$\alpha$ は Ω 上代数的で，Ω は K 上代数的だから α は K 上代数的である．したがって α は $K[X]$ の多項式 $g(X)$ の零点となっている：$g(\alpha)=0$．仮定によって $g(X)$ は Ω で 1 次式に分解されるから $\alpha \in \Omega$ である．故に $\Omega' = \Omega$．すなわち $\deg f = 1$ である．‖

証明 (定理 12.3 の証明)　$K[X]$ のモニック多項式のなす集合を整列して $\{f_\xi(X) \mid 0 < \xi < \alpha\}$ とする (α は順序数)．$K_0 = K$ とする．K の拡大の昇鎖列 K_ξ $(\forall \xi < \gamma)$ が構成されたとして，K_γ を合併体 $\bigcup_{\xi<\gamma} K_\xi$ 上の $f_\gamma(X)$ の最小分解体と定義する．そして

$$\Omega = \bigcup_{\xi<\alpha} K_\xi$$

と置くと，Ω が体をなし，K 上の代数拡大である (すなわち，Ω の元はすべて K 上代数的である) ことは超限帰納法によって明らかである．Ω が代数的に閉じていることは上の補題によって保証されている．‖

次の別証明も直観性に富む良い証明だと思うが，クラス版の極大原理を使うので，証明の前に付録「集合論のイロハ」§3 を参照していただきたい．

シュタイニッツの定理の別証明　K が無限体の場合を考える．宇宙 V (すなわち，すべての集合のなすクラス) の中で，体 K のすべての代数拡大体のなすクラスを考え，それを X とする．X には体の包含関係によって順序を入れることができる．体の拡大列の和集合は体をなすので，全順序をなす X の部分集合は上界を持つ．したがってクラス版の極大原理によって，X には極大元があるか，あるいは全順序をなす真のクラス Y $(\subsetneqq X)$ が存在する．

後者であるとして，上のような Y を取り，$L = \bigcup Y$ と置く．L の任意の元 α は定義によって K 上代数的である．すなわち

$$\exists f(X) \in K[X](f(\alpha)=0).$$

$K[X]$ の濃度は K の濃度に等しく，各 $f \in K[X]$ は def f 個以内の解しか持ち得ないから，$|L| = |K|$ が成り立つ．その結果，L は集合であるということが結論されるが，これは Y が真のクラスであるという仮定に反する．したがって，X に極大元 Ω が存在することになる．Ω が代数的に閉じていることは自明で，したがって K の代数的閉包である．

K が有限体の場合は L が可算無限濃度になることに注意すれば，他は同じである．∥

シュタイニツの業績は二重の意味で重要である．まず，その証明には整列原理が使われたという事実である．これが代数学にも explicit な形で選択公理 (と同値な命題) が登場した最初の場面である．(無自覚な形でなら，第 6 章で述べたように，頻繁に使われているのである．) この証明は整列原理なんて，数学とは無縁な，遠い世界の話だと思っていた数学界にセンセーションをもたらした．さらに，抽象的な代数学が登場したのはシュタイニツのこの業績が契機となったというのがもう一つの貢献である．抽象代数学の始まりというとエミー・ネーターやファン・デル・ヴェルデンを連想する人が多いだろうが，かれらの貢献は 1920 年代になってからである．公理的集合論の創始者の一人であるフレンケルも次のように述べている：

> It was a complete surprise for the mathematical world when in 1910 Steinitz called attention to the important task performed by the axiom of choice in algebra, both for certain problems of classical algebra and still more for abstract algebra, which became an important branch of mathematics through the influence of that very essay of Steinitz. ([18],p.77)

なお，ツォルン (1935 年) はシュタイニツの定理に今では良く知られた無限多変数多項式環を考察する証明を与えたが，これがツォルンの補題の由来である．その証明は，作られたイデアルが単位イデアルではないことを示すあ

たり自明とは言い難く，シュタイニツの証明の「簡易化」と称せるような代物ではない．この補題の重要性は言うまでもないが，ツォルンの名前を冠するのはどうかという疑義がしばしば呈されるのは，実際にはクラトフスキーを含む人たちによって大分前にこの命題が知られていたことが現在では判明しているからである．そういうわけで極大原理というのが内容から言っても適切であり，史実的にも偏らないので，本書ではこのように呼んでいる．

ところで，方程式論の基本定理は普通「代数学の基本定理」と呼ばれているけれども，実数体の連続性を使わずに証明することは出来ない．それに代数学の意味も 19 世紀と現代ではまったく異なっている．私はむしろ定理 12.3 こそ「代数学の基本定理」と呼ぶにふさわしい大定理だと思っていたが，そっくり同じことがフレンケルの本 [18] に書かれているのを知って意を強くした．

§2. K 共役写像

第 7 章では代数体 K から $\mathbb{Q}$ の代数的閉包 $\overline{\mathbb{Q}}$ の中への同型写像を考えて共役写像と呼んだが，以下ではこれを相対代数体の場合に拡張しよう．

K, L が代数体で $K \subsetneqq L$ のとき，L は K の**拡大体**，K は L の**部分体**と言い，L/K という記号で表す．(/ は商を表す記号ではなく，単に $K \subsetneqq L$ を意味していることに注意しよう.)　L/K の関係を**相対代数体**と呼び慣らわしている．

写像 $\sigma : L \longrightarrow \overline{\mathbb{Q}}$ が**中への** K **同型写像**であるとは

$$\sigma(x+y) = \sigma(x) + \sigma(y), \quad \sigma(xy) = \sigma(x)\sigma(y)$$

かつ

$$\sigma(a) = a \quad (\forall a \in K)$$

が成り立つことをいう．(体の準同型写像の場合，1 対 1 写像であることは必然的に成り立つので同型と仮定しなくても同じである.)

定義　中への K 同型写像 $\sigma : L \longrightarrow \overline{\mathbb{Q}}$ のことを L の K **共役写像**，あるいは L/K の共役写像という．また L の像 $\sigma(L)$ を L の K 上の**共役体**という．$\sigma(L)$ を σL，あるいは L^σ と書くことも多い．

[注意]　$\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数的閉包であるが，必然的に K の代数的閉包でもあることは，代数拡大の代数拡大は代数拡大であることから明らかである．記号で書けば，$\overline{K} = \overline{\mathbb{Q}}$.

$L = K(\theta)$ なる θ を取る．$n = [L : K]$ のとき，θ は K 上の n 次方程式

$$f(\alpha) = a_0 + a_1\theta + \cdots + a_n\theta^n = 0$$

を満たす．K 上の共役写像 σ をほどこすと

$$a_0 + a_1\theta^\sigma + \cdots + a_n(\theta^\sigma)^n = 0$$

を得るから θ^σ は $f(X) = 0$ の根 (つまり θ の共役根) である．また $\alpha \in L$ に対して

$$\alpha = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$$

と表せるから

$$\alpha^\sigma = c_0 + c_1\theta^\sigma + \cdots + c_{n-1}(\theta^\sigma)^{n-1}$$

が成り立つ．

$$f(X) = a(X - \theta^{(1)}) \cdots (X - \theta^{(n)}),\quad \text{ただし}\ \theta^{(1)} = \theta$$

と $\overline{\mathbb{Q}}$ において因数分解すれば $\theta^\sigma = \theta^{(j)}$ を満たすのだが，逆に任意の共役根 $\theta^{(j)}$ を取れば $\theta \rightsquigarrow \theta^{(j)}$ から K 同型写像 $K(\theta) \longrightarrow K(\theta^{(j)}) \subsetneqq \overline{\mathbb{Q}}$ が導かれる．実際，

$$K(\theta) \simeq K[X]/(f) \simeq K(\theta^{(j)})$$

だからである．したがって，$K(\theta^{(j)})$ が $K(\theta)$ の K 共役体のすべてであり，対応は $\sum_i c_i\theta^i \rightsquigarrow \sum_i c_i(\theta^{(j)})^n$ で与えられる．

L/K の共役写像 (j) を $K \subsetneqq M \subsetneqq L$ なる部分体 M に制限すると M/K の共役写像を得ることは共役写像の定義から自明だが，逆も成り立つ：

命題　M を L/K の中間体とする．M/K の任意の共役写像は L/K の共役写像に延長できる．

証明　$\tau : M \longrightarrow \overline{\mathbb{Q}}$ を K 共役写像とする．また $f(X)$ を $L = K(\theta)$ なる θ の満たす K 上の既約多項式とする．$L = M(\theta)$ でもあるから $M[X]/(g) \simeq M(\theta)$ を満たす M 上の既約多項式 $g(X)$ が存在する．$g(\theta) = 0$ だから $g|f$ である．$\varphi(X) \bmod g(X)$ に $\varphi^\tau(X) \bmod g^\tau(X)$ を対応させる写像によって $M[X]/(g) \simeq M^\tau[X]/(g^\tau)$ が得られる．そこで $g^\tau(\theta') = 0$ なる θ' を取ると $M^\tau[X]/(g^\tau) \simeq M^\tau(\theta')$ である．

一方 $g|f$ に τ をほどこしてみると $g^\tau|f$ がわかる．故に $\theta' = \theta^{(j)}$ なる (j) があるはずである．以上によって同型写像

$$\varphi : L = M(\theta) \simeq M^\tau(\theta^{(j)}) \subseteqq \overline{\mathbb{Q}}$$

が $\displaystyle\sum_{i=0}^{m-1} \alpha_i \theta^i \rightsquigarrow \sum_{i=0}^{m-1} \alpha_i^\tau (\theta^{(j)})^i$ なる対応から得られることがわかる（ここに $m = [L : M]$ である）．また $\varphi(\alpha) = \alpha^\tau$ $(\forall \alpha \in M)$ だから φ は τ の延長である．‖

この命題は次のように一般化することができる．

定理 12.4　M を体 K の拡大体とし，σ を M/K の共役写像とすると σ は K の代数的閉包 $\overline{K}$ の K 自己同型写像に延長できる．すなわち，(全射の)K 同型写像 $\sigma^* : \overline{K} \longrightarrow \overline{K}$ であって $\sigma^*|M = \sigma$ を満たすものが存在する．(ここに $\sigma^*|M$ は σ^* の M への制限写像を表す．)

写像を上の命題のように次々と拡大体に延長して行けば良いのだが，それだけでは「延長し終わる」ことは出来ないから，選択公理という超越的手段に頼らざるを得ない．σ のあらゆる延長の全体を考えると帰納的順序集合をなすので極大原理によって極大元がある．その極大元は上の命題を参考にすれば $\overline{K}$ の自己同型写像であることがわかる．この証明の細部をつめること，また次の系を示すことは訳のないことなので読者にお任せする．

系　体 K の代数的閉包は互いに K 上同型である．

§ 3. ガロア拡大の定義

定義　L/K を相対代数体とする．L/K の共役体 $L^{(j)}$ がすべて L に一致するとき $(L = L^{(j)})$，L は K 上 (あるいは L/K は) **ガロア拡大**であるといわれる．前節の考察に従えば，任意の $\varphi \in \mathrm{Aut}(\overline{\mathbb{Q}}/K)(= \overline{\mathbb{Q}}/K$ の自己同型写像の全体のなす集合) に対して $\varphi(L) = L$ が満たされることと言い換えられる．

なお，$\varphi(L) = L$ とか $L^{(j)} = L$ などは $\varphi(L) \subseteqq L, L^{(j)} \subseteqq L$ といっても同じことである．これは K 上の拡大次数を考えれば容易にわかることである．

例えば 2 次拡大 $L = K(\sqrt{a}), a \in K$ は常にガロア拡大である．これは $f(X) = X^2 - a = 0$ の解は $\pm\sqrt{a}$ で，ともに L の元だからである．

一方 $\mathbb{Q}(\sqrt[3]{2})$ は $\mathbb{Q}$ 上ガロア拡大ではない．それは $f(X) = X^3 - 2 = 0$ の解は

$$\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2} \qquad \left(\omega = \frac{-1+\sqrt{-3}}{2}\right)$$

だが $\sqrt[3]{2}$ 以外は $\mathbb{Q}(\sqrt[3]{2})$ に属しないからである．

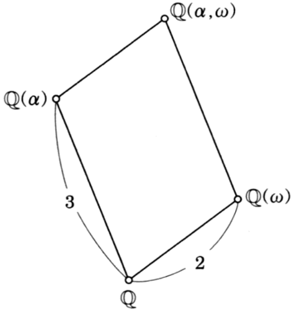
定理 12.5　L/K がガロア拡大であるためには，L において一つでも解を有する K 上の既約方程式はすべての解を L に持つことが必要十分である．

証明　L/K がガロア拡大であるとし，$g(X) \in K[X]$ を既約多項式としよう．$g(\alpha) = 0, \alpha \in L$ ならば他の解 α' も L の元であることを言えばよいが $K(\alpha) \subseteqq L$ によって前節の命題が適用できて，$\alpha' = \alpha^{(j)}$ となる L/K の共役写像 (j) が存在する．$L^{(j)} = K(\theta^{(j)}) = L$ がガロア拡大の仮定からわかるから $\alpha^{(j)} \in L$ である．逆は，ガロア拡大の定義から明らか．‖

定理 12.6　L/K の共役体 $L^{(1)}, \cdots, L^{(n)}$ の合併体 $L^{(1)} \cdots L^{(n)}(L^{(1)}, \cdots, L^{(n)}$ のすべてを含む最小の体) は K 上ガロア拡大である．したがって $L = K(\theta)$ のとき $K(\theta^{(1)}, \cdots, \theta^{(n)})$ は K 上ガロア拡大である．

証明　$\varphi \in \mathrm{Aut}(\overline{\mathbb{Q}}/K)$ を $F = K(\theta^{(1)}, \cdots, \theta^{(n)})$ の元に作用させる．φ は $\theta^{(1)}, \cdots, \theta^{(n)}$ を入れ換えるだけだから $\varphi(F) \subseteqq F$ は明らかである．故に F/K はガロア拡大である．‖

たとえば，$\sqrt[3]{2} = \alpha$ と置く．$\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ 上ガロア拡大ではなかったが，定理 12.6 によれば $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega)$ は $\mathbb{Q}$ 上ガロア拡大となる．



図には現れていないが $\mathbb{Q}(\alpha)$ の共役体である $\mathbb{Q}(\omega\alpha), \mathbb{Q}(\omega^2\alpha)$ も $\mathbb{Q}(\omega, \alpha)$ の部分体である．$\mathbb{Q}(\omega)$ の共役体は $\mathbb{Q}(\omega^2)$ でこれは $\mathbb{Q}(\omega)$ と一致している．たとえば $\alpha + \omega$ の $\mathbb{Q}$ 上の共役数は

$$\omega^i \alpha + \omega^j \quad (i = 0, 1, 2;\ j = 1, 2)$$

で計六つある．$\mathbb{Q}(\alpha, \omega)$ は $\mathbb{Q}$ 上 6 次だから $\alpha + \omega$ が原始要素，ω のかわりに $\sqrt{-3}$ をとっても同じことで $\theta = \sqrt[3]{2} + \sqrt{-3}$ と置くと，

$$\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\theta).$$

最小分解体は §1 でも定義したが，ガロア理論では重要だから再度掲げておこう：

定義　K を代数体，$f(X)$ を K 上の既約多項式とする．$f(X) = 0$ の解の全部 $\theta^{(1)}, \cdots, \theta^{(n)}$ を K に添加した体 $K(\theta^{(1)}, \cdots, \theta^{(n)})$ を $f(X) = 0$ の K

上の**最小分解体**という．最小分解体は定理 12.6 によってガロア拡大である．

問題　$M/K, L/M$ がともにガロア拡大でも L/K はガロア拡大ではない例を作れ．

[答の例]　$L=\mathbb{Q}(\sqrt[4]{2})$, $M=\mathbb{Q}(\sqrt{2})$, $K=\mathbb{Q}$ を考えよ．

問題　L_1, L_2 が K 上ガロア拡大ならば L_1L_2 も K 上ガロア拡大であることを示せ．

§ 4. ガロアの理論

L/K を代数体 K のガロア拡大とする．$L^{(j)}=L$ であるから L の K 上の共役写像の全体は L/K の**自己同型写像** (すなわち L から L への K 同型写像) の全体と一致する．この L/K の自己同型写像の全体を $G(L/K)$ と記す．

$\sigma \in G(L/K), \tau \in G(L/K)$ に対して積 $\sigma\tau \in G(L/K)$ を

$$(\sigma\tau)(x)=\sigma(\tau(x)) \quad (\forall x \in L)$$

によって定義する．

問題　$G(L/K)$ は群をなす．これを証明せよ．

定義　ガロア拡大 L/K の K 自己同型写像の全体 $G(L/K)$ のなす群を L/K の**ガロア群** (Galois group) と呼ぶ．ガロア群 $G(L/K)$ がアーベル群のとき L/K は**アーベル拡大**，また巡回群のとき**巡回拡大**，であると言う．

例題　$x^3-2=0$ の最小分解体 $K=\mathbb{Q}(\alpha,\beta)$，ここに $\alpha=\sqrt[3]{2}, \beta=\sqrt{-3}$, の $\mathbb{Q}$ 上のガロア群を決定せよ．

解答　$[K:\mathbb{Q}]=6$ だから $G=G(K/\mathbb{Q})$ の位数は 6 である．G の元は α を $\omega^k\alpha$ $(k=0,1,2)$ のいずれかへ，β を $\pm\beta$ のいずれかへ写すから計 6 通りの可能性があるが，$|G|=6$ より，これらのすべてが起り得る．$\sigma \in G, \tau \in$

G を

$$\sigma(\alpha) = \omega\alpha, \quad \sigma(\beta) = \beta,$$
$$\tau(\alpha) = \alpha, \quad \tau(\beta) = -\beta$$

によって定まる K の自己同型写像とする．まず

$$\sigma^3 = e, \quad \tau^2 = e \tag{1}$$

がわかる．さらに $(\sigma\tau)(\alpha) = \sigma\alpha = \omega\alpha$, $(\sigma\tau)(\beta) = \sigma(-\beta) = -\beta$ などの計算をして

$$\sigma\tau = \tau\sigma^2, \quad \sigma^2\tau = \tau\sigma \tag{2}$$

がわかる．したがって $G = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ は関係 (1), (2) を持った群である．なお，ちょっと調べれば $G \simeq S_3$(3 次対称群) であることがわかる．

このように添加する元がわかっている場合にはガロア群の決定はさして難しくはないが，単に $f(X) = 0$ が与えられたとき最小分解体のガロア群を求めよ，と要求されてもおいそれと求まるものではない．つぎの問題は中ではもっとも簡単な部類である：

問題　$X^4 - X^2 + 1 = 0$ の $\mathbb{Q}$ 上の最小分解体のガロア群を決定せよ．

[ヒント]　$X^4 - X^2 + 1 = (X^2+1)^2 - 3X^2$ と変形すれば容易に解が求まる．最小分解体は $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ である．

問題　1 の n 乗根は K に含まれているものとし，ζ を 1 の原始 n 乗根の一つとする．すなわち $m < n$ ならば $\zeta^m \neq 1$ であるとする．$a \in K$ かつ $[K(\sqrt[n]{a}) : K] = n$ のとき $K(\sqrt[n]{a})/K$ は n 次巡回拡大であることを示せ．

問題　体 M がガロア拡大 L/K の中間体 (つまり $K \subseteqq M \subseteqq L$) であれば L/M もガロア拡大で，そのガロア群は G の元で M の各元を動かさないものの全体である：

$$G(L/M) = \{\sigma \in G(L/K) \mid \sigma x = x (\forall x \in M)\}$$

[ヒント]　σ を L/M の共役写像として $\sigma L \subseteqq L$ を示せばよいが，$K \subseteqq M$ によって σ は L/K の共役写像でもある．したがって $\sigma \in G(L/K)$.

基本定理の証明の前に補題を一つ準備する．

補題　L/K をガロア拡大とする．また L の自己同型写像 (K 同型とは限らない) の全体のなす群を $\mathrm{Aut}(L)$ と記す．$\mathrm{Aut}(L)$ の部分群 H に対して

$$L^H = K \Longleftrightarrow H = G(L/K)$$

が成り立つ．ここに $L^H = \{x(\in L) \mid \tau x = x \quad (\forall \tau \in H)\}$ とする．L^H は H の**固定体**と呼ばれる．

証明　まず $H = G(L/K)$ が成り立つとしよう．ガロア群の定義から $K \subseteqq L^H$ は明らかである．

$$H \subseteqq G(L/L^H) \subseteqq G(L/K)$$

によって $G(L/K) = G(L/L^H)$ を得るが，一方 $|G(L/K)| = [L:K]$，また $|G(L/L^H)| = [L^H:K]$ だから，これは $L^H = K$ を示している．

逆に $L^H = K$ としよう．まずガロア群の定義によって $H \subseteqq G(L/K)$ である．故に

$$|H| \leqq |G(L/K)|$$

今 $L = K(\theta)$ として，

$$F(X) = \prod_{\sigma \in H} (X - \theta^\sigma)$$

と置けば，$F(X)$ の係数 $\in L^H = K$ である．しかも $F(\theta) = 0$ だから $F(X)$ は θ の満たす既約方程式で割り切れる．故に，$[L:K] \leqq \deg F = |H|$．

$$\therefore \quad |G(L/K)| \leqq |H|$$

以上によって $|H| = |G(L/K)|$ が示された．故に $H = G(L/K)$ である．　‖

定理 12.7 (ガロアの基本定理)　L/K をガロア拡大とし，$G = G(L/K)$ とする．G の部分群 H に対してその固定体 L^H を対応させる写像は G の部分群全体のなす集合と L/K の中間体全体のなす集合との間の全単射を与える．またその逆写像は $M \rightsquigarrow G(L/M)$ である．

証明　一般に写像 $S : A \longrightarrow B$ が全単射であるためには，$T \circ S$ が A 上の恒等写像，かつ $S \circ T$ が B 上の恒等写像となる $T : B \longrightarrow A$ が存在することを示せばよいので，今の場合，

$$G(L/L^H) = H$$

および

$$L^{G(L/M)} = M$$

を示せばよい．補題において $L^H = M$ と置くと $H = G(L/M)$ が得られる．次に $H = G(L/M)$ と置くと $L^H = M$ が得られる．∥

上の全単射がいわゆる**反変的**である，すなわち，

$$H_1 \subsetneqq H_2 \Longleftrightarrow L^{H_1} \supsetneqq L^{H_2}$$

が成り立つことは明らかである．

系 1　(1)　M をガロア拡大 L/K の中間体とすると

$$G(L/\sigma M) = \sigma G(L/M)\sigma^{-1} \quad (\forall \sigma \in G(L/K))$$

(2)　H を $G(L/K)$ の部分群とすると

$$\sigma(L^H) = L^{\sigma H \sigma^{-1}} \quad (\forall \sigma \in G(L/K))$$

証明　(1) を示そう．(2) は演習とする．

$$\begin{aligned} \tau \in G(L/\sigma M) &\Longleftrightarrow \tau(\sigma x) = \sigma x \quad (\forall x \in M) \\ &\Longleftrightarrow (\sigma^{-1}\tau\sigma)x = x \quad (\forall x \in M) \\ &\Longleftrightarrow \sigma^{-1}\tau\sigma \in G(L/M) \\ &\Longleftrightarrow \tau \in \sigma G(L/M)\sigma^{-1} \end{aligned}$$ ∥

系 2　M をガロア拡大 L/K の中間体とする．M/K がガロア拡大であるためには $G(L/M)$ が $G(L/K)$ の正規部分群をなすことが必要十分である．このとき自然な対応によって

$$G(M/K) \simeq G(L/K)/G(L/M)$$

が成り立つ．

証明　前半は系 1(1) あるいは (2) から明らか．写像 $\varphi : G(L/K) \longrightarrow G(M/K)$ を σ に対して σ の制限 $\sigma|M$ を対応させるものとしよう．全射性は写像の延長可能性からわかる．φ の核は $\sigma|M =$ 恒等写像，すなわち $\sigma \in G(L/M)$ なる σ からなる．‖

系 3　L/K をガロア拡大とする．$H_1 \cup H_2$ を H_1, H_2 を含む最小の群，また $M_1 \cup M_2$ を M_1, M_2 を含む最小の体を表す記号とすれば，

(1) H_1, H_2 を $G(L/K)$ の部分群とする．このとき

$$G(L/M_1 \cap M_2) = H_1 \cup H_2, \quad L^{H_1 \cup H_2} = M_1 \cap M_2$$

が成り立つ．

(2) $M_i = G(L/M_i)$ $(i = 1, 2)$ とすると

$$G(L/M_1 \cup M_2) = H_1 \cap H_2, \quad L^{H_1 \cap H_2} = M_1 \cup M_2$$

が成り立つ．

問題　系 3 を証明せよ．

代数や整数論では $H_1 \cup H_2, M_1 \cup M_2$ という記号を系 3 の意味ではあまり使わないが，誤解さえしなければ印象的であろう．

例　$\mathbb{Q}(\alpha, \beta)$, $\alpha = \sqrt[3]{2}$, $\beta = \sqrt{-3}$ とする．$\mathbb{Q}(\beta)$ は $\mathbb{Q}$ 上ガロア拡大である．$\mathbb{Q}(\beta)$ に対応する $G = \{\sigma^i \tau^j \mid i = 0, 1, 2;\ j = 0, 1\}$ の部分群 N は $\{e, \sigma, \sigma^2\}$ である．$\tau\sigma^2\tau^{-1} = \sigma$, $\tau\sigma\tau^{-1} = \sigma^2$ だから，たしかに N は G の正規部分群である．$\mathbb{Q}(\alpha)$ に対応する部分群 H は $\{e, \tau\}$ である．また

$$\sigma H \sigma^{-1} = \{e, \tau\sigma\}$$

である．

$$(\tau\sigma)(\omega\alpha) = \omega\alpha$$

だから $\sigma H \sigma^{-1}$ の固定体は $\mathbb{Q}(\omega\alpha)$ である．$\mathbb{Q}(\omega^2\alpha)$ に対応する群は $\sigma^2 H \sigma^{-2} = \{e, \tau\sigma^2\}$ である．

定理 12.8　1 の原始 n 乗根の一つを ζ とし，$\zeta \in K$ とする．L/K が n 次巡回拡大であれば

$$L = K(\sqrt[n]{a})$$

を満たす $a \in K$ が存在する．

証明　$G(L/K)$ の生成元を σ とする．$x \in L$ に対して

$$y = \sum_{j=0}^{n-1} \zeta^{-j} \sigma^j(x)$$

と置く．

$$\begin{aligned} \sigma y &= \sum_{j=0}^{n-1} \zeta^{-j} \sigma^{j+1}(x) = \zeta \sum_{j=0}^{n-1} \zeta^{-j-1} \sigma^{j+1}(x) \\ &= \zeta \sum_{j=1}^{n} \zeta^{-j} \sigma^j(x) = \zeta y \quad (\because\ \sigma^n = e, \zeta^n = 1) \end{aligned}$$

仮りに $y \neq 0$ となる $x \in L$ が存在するとしよう．$K(y) \subseteq L$ であるが $K(y)$ に対応する $G(L/K)$ の部分群は $\sigma y = \zeta y$ によって $\{e\}$ である．すなわち $K(y) = L$．しかも $a = y^n$ と置くと $\sigma a = (\sigma y)^n = (\zeta y)^n = y^n = a$ $\therefore$ $\sigma a = a$．故に $a \in K$ を得る．

さて仮りに $L = K(\theta)$ となる θ に対して

$$\sum_{j=0}^{n-1} \zeta^{-j} \sigma^j(\theta^k) = 0$$

が $k = 0, 1, \cdots, n-1$ のいずれについても成り立つとする．これを連立 1 次方程式と考えると非自明解 $1, \zeta^{-1}, \cdots, \zeta^{-n+1}$ を持つから $\det \sigma^j(\theta^k) = 0$ だが，$\sigma^j(\theta^k) = (\sigma^j\theta)^k$ によって

$$\det(\sigma^j\theta^k) = \prod_{j>i} (\sigma^j\theta - \sigma^i\theta) = 0$$

である．$\sigma^j\theta \neq \sigma^i\theta$ だから，これは矛盾．‖

§ 5.　一般代数方程式と対称式の基本定理

定義　n 変数の有理式 $F(X_1, \cdots, X_n) \in \mathbb{Q}(X_1, \cdots, X_n)$ が $X_1, \cdots, X_n$ に関して**対称**であるとは

$$\sigma F = F \quad (\forall \sigma \in S_n)$$

が成り立つことを言う．

ここに $\sigma F(X_1, \cdots, X_n) = F(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$ である．要するに，有理対称式とはどんな風に変数を入れ換えても不変な有理式 (すなわち，(多項式)÷(多項式) で表される関数) のことである．たとえば，

$$(\alpha-\beta)^2 = (\alpha+\beta)^2 - 4\alpha\beta,$$
$$\alpha^3+\beta^3+\gamma^3 = (\alpha+\beta+\gamma)^3 - 3(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha) + 3\alpha\beta\gamma$$

といった変形は高校数学でも常識であるが，こういう変形の暗示するところは，対称式は必ず，2 変数の場合は $\alpha+\beta$, $\alpha\beta$, 3 変数の場合は $\alpha+\beta+\gamma$, $\alpha\beta+\beta\gamma+\gamma\alpha$, $\alpha\beta\gamma$ という，いわゆる基本対称式によって表現できるということである．このことは高校数学では証明されてはいないが，よく出題されることによって当然のことと暗黙のうちに了解されている．しかし，それを厳密に証明せよと要求されると読者もちょっと途方に暮れるだろう．対称式は基本対称式で表せるという命題 (対称式に関する基本定理) は 18 世紀にウェアリングによって証明された有名な定理である．本節ではガロア理論の応用例として証明してみよう．この定理は元来ラグランジュやガロアの古典的な方程式論の中では基本的な役割を果たすのだが，現在では対称式論を使わず，別の基礎付けによってガロアの理論が組み立てられているから，循環論法というわけではない．

定義　X の n 次多項式 $(X+x_1)(X+x_2)\cdots(X+x_n)$ の係数，すなわち

$$\sum_i x_i, \quad \sum_{i<j} x_i x_j, \quad \cdots, \quad \prod_i x_i$$

を $x_1, x_2, \cdots, x_n$ の**基本対称式**という．

定理 12.9　変数 $x_1, x_2, \cdots, x_n$ の有理対称式は基本対称式の有理式として表される．

証明　$L = \mathbb{Q}(x_1, \cdots, x_n)$，すなわち n 変数の有理関数の全体のなす体 (n 変数有理関数体) を L とする．

$\sigma \in S_n, f \in L$ に対して

$$(\sigma f)(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$$

と定義されているから $\sigma \in \mathrm{Aut}(L)$(= 自己同型写像の全体のなす群) とみなせる．故に $S_n \subseteqq \mathrm{Aut}(L)$ である (S_n は n 次対称群を表す)．そこで $x_1, \cdots, x_n$ の基本対称式を $a_1, \cdots, a_n$ とする．このとき

$$\begin{aligned} F(X) &= X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \\ &= (X + x_1)(X + x_2) \cdots (X + x_n) \end{aligned}$$

であるから，L は $K = \mathbb{Q}(a_1, \cdots, a_n)$ 上 $F(X) = 0$ の根を添加した体なので $F(X) = 0$ の最小分解体である．したがって，L/K はガロア拡大である．(ガロアの理論は代数体で説明してきたが，何の変更もなく，関数体の場合に使える．読者は自分でこのことをチェックしてほしい．)　さらに $\sigma \in S_n$ は K の元を動かさないから，$S_n \subseteqq G(L/K)$ である．故に，

$$|S_n|(= n!) \leqq |G(L/K)| = [L : K]$$

である．一方，$F(X)$ の次数は n なので $[L : K] \leqq n!$ である．($G(L/K)$ は，根 $x_1, \cdots, x_n$ の置換のなす群なので，S_n の部分群だからである．)　したがって，$[L : K] = n!$ となり，

$$\mathrm{Gal}(L/K) = S_n$$

を得る．ガロアの基本定理によって $K = L^{S_n}$ が成り立つが，これは有理対称関数が $K = \mathbb{Q}(a_1, \cdots, a_n)$ の元，すなわち基本対称式の有理関数であることを示している． ‖

この定理は対称多項式が基本対称式の多項式として表せることまでは保証していない．それはこれから示すことである．

次に，逆に独立な変数 $a_1, \cdots, a_n$ が与えられたとして，これらを係数とする方程式

$$F(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

を考える．これを n 次の**一般代数方程式**という．方程式 $F(X) = 0$ の $K = \mathbb{Q}(a_1, \cdots, a_n)$ 上のガロア群 (すなわち，最小分解体 L/K のガロア群) は定

理 12.9 の証明から容易に想像がつくように S_n となるであろう．これを証明しておこう．

定理 12.10　n 次の一般代数方程式のガロア群は S_n である．

証明　$K=\mathbb{Q}(a_1,\cdots,a_n)$ とし，K 上 $F(X)=0$ の最小分解体を L とすれば，

$$F(X)=(X+x_1)(X+x_2)\cdots(X+x_n),\quad x_1,\cdots,x_n\in L$$

と分解され (今度は $x_1,\cdots,x_n$ は独立変数ではない)，

$$L=K(x_1,\cdots,x_n)=\mathbb{Q}(x_1,\cdots,x_n)$$

が成り立つ ($a_i\in\mathbb{Q}(x_1,\cdots,x_n)$ だからである)．

一方で，$\mathbb{Q}$ 上の n 変数有理関数体 $L^*=\mathbb{Q}(x_1^*,\cdots,x_n^*)$ を考え，

$$\begin{aligned}F^*(X)&=(X+x_1^*)(X+x_2^*)\cdots(X+x_n^*)\\&=X^n+a_1^*X^{n-1}+\cdots+a_n^*\end{aligned}$$

(ここで $a_1^*,\cdots,a_n^*$ は $x_1^*,\cdots,x_n^*$ の基本対称式) と置けば，定理 12.9 の証明で見たように L^* は $K^*=\mathbb{Q}(a_1^*,\cdots,a_n^*)$ 上の $F^*(X)=0$ の最小分解体で，そのガロア群 $G(L^*/K^*)$ は S_n と同型である．したがって，同型写像 $\varphi:L^*\longrightarrow L$ で $\varphi(K^*)=K$ を満たすものが存在することを示せば，必然的に

$$G(L^*/K^*)\simeq G(L/K)$$

が成り立ち，定理が証明されたことになる．

$\mathbb{Q}[x_1^*,\cdots,x_n^*]$ は多項式環であるから，$f(x_1^*,\cdots,x_n^*)\rightsquigarrow f(x_1,\cdots,x_n)$ によって上への準同型写像

$$\varphi:\mathbb{Q}[x_1^*,\cdots,x_n^*]\longrightarrow\mathbb{Q}[x_1,\cdots,x_n]$$

が定義される．このとき $\varphi(a_i^*)=a_i$ である．さらに $\mathbb{Q}[a_1,\cdots,a_n]$ が多項式環であるから $g(a_1,\cdots,a_n)\rightsquigarrow g(a_1^*,\cdots,a_n^*)$ によって準同型写像 ψ : $\mathbb{Q}[a_1,\cdots,a_n]\longrightarrow\mathbb{Q}[a_1^*,\cdots,a_n^*]$ が定義され，$\varphi\circ\psi=$ 恒等写像である．また $\mathbb{Q}[a_1^*,\cdots,a_n^*]$ 上に制限すれば $\psi\circ\varphi=$ 恒等写像が成り立つ．したがって ψ は同型写像である．この同型写像は商体同士の同型写像 $\psi:K\simeq K^*$ に延長

される．特に $F(X)$ に対して $\psi F(X) = F^*(X)$ だから，ψ は $F(X), F^*(X)$ の最小分解体である L, L^* 間の同型写像 $\psi : L \longrightarrow L^*$ に延長される．これによって $G(L/K) \simeq G(L^*/K^*)$ が証明された． ‖

次節で説明するように，代数方程式の解が係数から冪根を使って表せるための条件はそのガロア群が可解群であることである．ところが $n \geqq 5$ のとき S_n は可解ではないから，$n \geqq 5$ のときは一般代数方程式 (文字係数の方程式) はいわゆる「解の公式」を持たない，つまり係数から作られる数の開冪では解を表せないのである．

系 1　$x_1, \cdots, x_n$ を独立変数とし，$a_1 = \sum_i x_i, \cdots, a_n = \prod_i x_i$ を n 変数の基本対称式とすると $\mathbb{Q}[a_1, \cdots, a_n]$ は多項式環 $\mathbb{Q}[x_1, \cdots, x_n]$ と同型である．

証明は定理 12.10 の証明に含まれている．

系 2 (対称式の基本定理)　任意の対称多項式は基本対称式の多項式として表せる．

証明　$f(x_1, \cdots, x_n)$ を対称多項式とすると定理 12.10 によって

$$f = \frac{g}{h}, \quad g, h \in \mathbb{Q}[a_1, \cdots, a_n]$$

と表せることはわかっている．すなわち

$$f \cdot h = g$$

であるが，$\mathbb{Q}[a_1, \cdots, a_n]$ は U.F.D. だから (系 1 と定理 7.4 による) g と h とは $\mathbb{Q}[a_1, \cdots, a_n]$ の元として互いに素 (つまり，公約素元を持たない) としてよい．

$\mathbb{Q}[x_1, \cdots, x_n]$ の元はすべて $\mathbb{Q}[a_1, \cdots, a_n]$ 上整である．つまり，$\mathbb{Q}[a_1, \cdots, a_n]$ の元を係数に持つモニック方程式の解である．なぜなら $x_1, \cdots, x_n$ それぞれが $\mathbb{Q}[a_1, \cdots, a_n]$ 上整だから，これらの積和はやはり整であるからであ

る．さて $f \in \mathbb{Q}[x_1, \cdots, x_n]$ だから今の議論により

$$f^k = c_1 f^{k-1} + c_2 f^{k-2} + \cdots + c_k \quad (c_1, \cdots, c_k \in \mathbb{Q}[a_1, \cdots, a_n])$$

と表せる．$f = g/h$ だから

$$g^k = h(c_1 g^{k-1} + c_2 h g^{k-2} + \cdots + c_k h^{k-1})$$

ところで系 1 によって $\mathbb{Q}[a_1, \cdots, a_n]$ は U.F.D. であるから，上式は $h = 1$(正確には，$h \in \mathbb{Q}$) を示している．すなわち $f \in \mathbb{Q}[a_1, \cdots, a_n]$．∥

証明の最後の個所は $\mathbb{Q} \cap \mathbb{O} = \mathbb{Z}$(定理 7.3) の証明と同じパターンである．言い換えれば，n 変数多項式環は整閉である．これは U.F.D. 一般に言えることである．

多項式環 $\mathbb{Q}[X_1, \cdots, X_n]$ がネーター環であること (すなわち，極大条件を満たすこと) も知られている (ヒルベルトの基底定理)．だから 2 変数以上の多項式環がデデキント環にならない理由は唯一つ，「素イデアル = 極大イデアル」という条件が満たされないことである．

§ 6. 代数方程式の可解性

K を代数体とするとき定理 12.8 によれば $\alpha \in K$ に対して $K(\sqrt[n]{\alpha})/K$ は 1 の原始 n 乗根 $\zeta \in K$ のときには巡回拡大になるのであった．したがって，1 の冪根 ζ を添加した体 $K(\zeta)/K$(円分体と呼ばれる) が常に累開冪拡大であることを示せれば，K 上の既約方程式 $f(X) = 0$ が累開冪的に (すなわち，開冪を重ねて) 解けるためには，$f(X)$ の K 上の最小分解体のガロア群 G が

$$G_0(= \{e\}) \subsetneqq G_1 \subsetneqq \cdots \subsetneqq G_{m-1} \subsetneqq G_m(= G) \tag{3}$$

ただし，各 G_j は G_{j+1} の正規部分群で G_{j+1}/G_j は巡回群である，という部分群 G_j の列を持つことが条件となるのではないかと予想される．これを本節では証明しよう．

まず円分体が累開冪拡大であることを示そう．「1 の n 乗根は $\sqrt[n]{1}$ だから冪根で表せているではないか」と言ってはいけません．こういうあいまいさ

を封ずるために開冪拡大の問題では 2 項方程式 $x^n - a = 0$ はいつも既約であると仮定することにしよう．このとき 1 の原始 n 乗根，たとえば $e^{2\pi i/n}$ が累開冪的に表せるか，これが問題である．

証明に先立ち，定義を与えておこう．

定義　有限群 G は (3) のような部分群の列 $\{G_j\}_{j=0}^{n}$ (各 G_{j+1}/G_j は巡回群) を持つとき，**可解群**と呼ばれる．

問題　次を示せ：

1. 可解群 G の部分群も可解群である．
2. N を可解群 G の正規部分群とすれば商群 G/N も可解群である．
3. G を有限群，N をその正規部分群とする．N と G/N が共に可解群ならば G 自身も可解群である．

定義

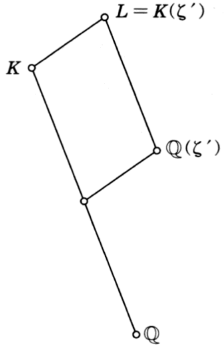
$$K = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_m = L, \quad K_{j+1} = K_j(\sqrt[n_j]{\alpha_j}) \quad (\alpha_j \in K_j)$$

なる体の列が取れるとき，拡大 L/K は**累開冪的**であるという．また K 上既約な $f(X)$ の最小分解体を含む累開冪拡大 L/K が存在するとき，$f(X) = 0$ は K 上**代数的に可解**という．

定理 12.11 (円分方程式の可解性)　K を代数体，ζ を 1 の冪根とすると $\mathbb{Q}(\zeta)/\mathbb{Q}$ は累開冪拡大である．

証明　ζ が 1 の原始 n 乗根であるとして，n に関する累積帰納法を適用する．$n = 1, 2$ なら $\mathbb{Q}(\zeta) = \mathbb{Q}$ だから証明することがない．今与えられた n より小さい自然数については定理が示されているとしよう．このとき $\varphi(n) < n$ であるから仮定によって，1 の原始 $\varphi(n)$ 乗根 ζ' に対して $\mathbb{Q}(\zeta')/\mathbb{Q}$ は累開冪拡大である (次ページの図を参照すると良い)．

1 の原始 n 乗根 ζ を $\mathbb{Q}$ に添加した体を K とする：$K = \mathbb{Q}(\zeta)$.



$K/\mathbb{Q}$ は第 13 章の定理 13.2 によって位数 $\varphi(n)$ のアーベル群をガロア群に持つ．したがって当然可解である．$L=K(\zeta')$ とすると，次に述べる補題によって $G(L/\mathbb{Q}(\zeta'))$ も可解群である．$\zeta'\in\mathbb{Q}(\zeta')$ だから，定理 12.8 によって $L/\mathbb{Q}(\zeta')$ は累開冪拡大である．$\mathbb{Q}(\zeta')/\mathbb{Q}$ は累開冪拡大だったから，$L/\mathbb{Q}$ は累開冪拡大である．これで定理が証明された．‖

補題　(**ガロア拡大の推進定理**)　L/K をガロア拡大，M/K を有限次拡大とする．このとき LM/M もガロア拡大で，

$$G(LM/M)\simeq G(L/L\cap M)$$

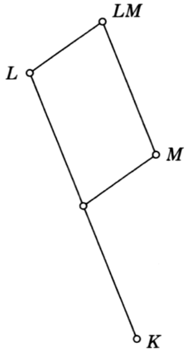
が成り立つ (次ページの図参照).

証明　(図を参考にすると良い)　$L=K(\theta)$ ならば $LM=M(\theta)$ だから LM/M がガロア拡大であることは明らかである．$\sigma\in G(LM/M)$ に対し，σ の L への制限 $\sigma|L$ を考えると，$\sigma|L\in G(L/L\cap M)$ が成り立つ．この写像を φ とすれば，φ は単射である．さらに $\tau\in G(L/L\cap M)$ を任意に取ると，$\tau'(x)=x$ $(\forall x\in M)$, $\tau'(y)=\tau(y)$ $(\forall y\in L)$ と定義することによって，$\tau'|L=\tau$ なる $\tau'\in G(LM/M)$ が定まるので φ は全射でもある．‖

定理 12.12　体 K 上の既約方程式 $f(X)=0$ が代数的に可解であるため

には，$f(X)$ の最小分解体のガロア群が可解群なることが必要十分である．

証明　$f(X)$ の最小分解体を L とし，L/K のガロア群を G とする：$G = G(L/K)$．



$n = [L:K]$ として 1 の原始 n 乗根を ζ，そして $M = K(\zeta)$ とする．

G が可解群であると推進定理によって LM/M もガロア拡大で，$G(LM/M)$ も可解群である (p.205 の問題の 1.)．$\zeta \in M$ だから LM/M は累開冪拡大である．また M/K も累開冪拡大である (定理 12.11)．故に LM/K は累開冪拡大だが，$L \subsetneqq LM$ なので，$f(X) = 0$ は K 上代数的に可解である．

逆に $f(X) = 0$ が代数的に可解，すなわちある累開冪拡大 L/K があって $L' \subsetneqq L$ (L' は $F(X)$ の最小分解体) であるとする．K 上の累開冪拡大の K 共役体はまた K 上累開冪拡大だから，これらを合併して L/K 自身が K 上ガロア拡大であるとしてもよい．そこで

$$K = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_{s-1} \subsetneqq K_s = L,$$
$$K_{i+1} = K_i(\sqrt[n_i]{a_i}), \quad a_i \in K_i$$

なる L の部分体 K_i の列を取る．$n_i (i = 0, \cdots, s-1)$ の最小公倍数を n とせよ．ζ を 1 の原始 n 乗根とし，$M = K(\zeta)$ とすれば，$G(LM/M)$ が可解群で，しかも $G(M/K)$ が可解群なので $G(LM/K)$ は可解群である (問題の 3.)．$L' \subsetneqq LM$ なので $G(L'/K)$ も可解群である (問題の 2.)．　‖

系　一般代数方程式は次数が 5 以上のとき代数的に可解ではない．すなわち冪根を用いる解の公式は存在しない．

定理 12.10 によって一般 n 次方程式は S_n をガロア群として持つが，S_n の部分群 A_n(交代群) は $n \geqq 5$ のとき単純群であって可解群ではないからである．(この事実の証明は群論，あるいは代数学の教科書に任せる．)

文字係数の一般代数方程式ではなくても，可解でない方程式の例は簡単に作れる．たとえば，

$$X^5 - X - 1 = 0$$

のガロア群は S_5 である．

5 次以上の方程式に解がないわけではないから，解を何らかの関数で表すことは古来試みられてきた．たとえば 5 次方程式の解は楕円モジュラー関数を使って表現できる (エルミートによる)．さらに高次の方程式についても研究がある．そもそも

$$\sqrt[n]{a} = e^{\frac{1}{n}\log a}$$

であるし，1 の n 乗根は $e^{2\pi i/n}$ であるから，4 次以下の方程式が指数関数 e^z という周期関数を使って解が表せていることを考えれば，5 次方程式が楕円関数という 2 重周期関数を用いて解くことが出来ても，驚くには当たらない．ガウスが既にこの事実に気付いていることにアーベルは着目していた，というような逸話は数学史の方ではよく知られている．

第13章　ヒルベルトの理論

代数体 K のガロア拡大 L において基礎体 K の素イデアルがどのように分解するかをガロア群との関係で記述するヒルベルトの理論は類体論以前の代数的整数論の精華である．イデアル論とガロア理論の結びつきの美しさに魅せられて代数的整数論を専攻したと聞いている先輩方も多い．本章では，類体論を理解するのに必要な範囲で，ヒルベルトの理論を紹介しよう．

§1. 円分体

円分体論は類体論のひな型である．つまり，「$\mathbb{Q}$ 上の類体論」＝「円分体論」である．この $\mathbb{Q}$ 上の類体論を展開するのに必要な土台をここで築くことにしよう．

自然数 m に対して 1 の原始 m 乗根を ζ_m，しばしば略して ζ と記す．一例として $\zeta = e^{2\pi i/m}$ が 1 の原始 m 乗根である．まず ζ を $\mathbb{Q}$ に添加した体 $\mathbb{Q}(\zeta)$ が $\mathbb{Q}$ 上ガロア拡大であることを見よう．

ζ に $\mathbb{Q}(\zeta)$ の共役写像 σ をほどこせば $(\zeta^\sigma)^m = (\zeta^m)^\sigma = 1$ だから，ζ^σ も 1 の m 乗根である．1 の m 乗根は $1, \zeta, \zeta^2, \cdots, \zeta^{m-1}$ で尽くされるから $\zeta^\sigma \in \mathbb{Q}(\zeta)$．したがって $\mathbb{Q}(\zeta)/\mathbb{Q}$ はガロア拡大である．ζ が 1 の原始 m 乗根ならば ζ^σ も 1 の原始 m 乗根である．($\because$ $(\zeta^\sigma)^k = 1 \Longleftrightarrow (\zeta^k)^\sigma = 1 \Longleftrightarrow \zeta^k = 1$.) ところで ζ^k が 1 の原始 m 乗根である条件は $(k, m) = 1$ であるから，1

の原始 m 乗根は $\varphi(m)$ 個あることになる．そこで

$$\Phi_m(X) = \prod_{(k,m)=1} (X - \zeta^k)$$

と置く．上式の両辺に $\mathbb{Q}(\zeta)/\mathbb{Q}$ の自己同型写像をほどこしても不変であるから $\Phi_m(X) \in \mathbb{Q}[X]$ がわかる．ζ^k はすべて代数的整数なので $\mathbb{O} \cap \mathbb{Q} = \mathbb{Z}$ によって実は $\Phi_m(X) \in \mathbb{Z}[X]$ である．

問題　$X^m - 1 = \prod_{d|m} \Phi_d(X)$ を示せ．

[ヒント]　1 の原始 d 乗根の全体の集合を M_d とすると $\bigcup_{d|m} M_d$ は 1 の m 乗根の全体のなす集合である．

定義　$\Phi_m(X)$ を**円周等分多項式**，略して**円分多項式**という．

たとえば素数 p に対しては

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

である．これが既約であることはアイゼンシュタインの判定法というのがあって証明できるのだが，実は一般に次が成り立つ：

定理 13.1　円分多項式 $\Phi_m(X)$ は $\mathbb{Q}$ 上既約である．

証明　いま

$$\Phi_m(X) = F(X) \cdot G(X), \quad F(X), G(X) \in \mathbb{Z}[X], \quad \text{かつモニック}$$

と因数分解されて，一つの 1 の原始 m 乗根 ζ が $F(\zeta) = 0$ を満たしていると仮定する．他の 1 の原始 m 乗根は ζ^a (ただし $(a,m) = 1$) と表せるが，これらが $G(X) = 0$ の根となることはないことを示せばよい．それには任意の素数 p (ただし $p \nmid m$) に対して $F(\zeta^p) = 0$ であることを示せば十分である．

仮りに $G(\zeta^p) = 0$ としよう．$K = \mathbb{Q}(\zeta)$ の整数環 $\mathbb{O}_K$ における p の上にある素イデアルを一つ取って $\mathfrak{p}$ とする．

$$G(X^p) \equiv G(X)^p \pmod{\mathfrak{p}}$$

であるから $G(\zeta)^p \equiv 0 \pmod{\mathfrak{p}}$. 故に $G(\zeta) \equiv 0 \pmod{\mathfrak{p}}$. 一方 $F(\zeta) \equiv 0 \pmod{\mathfrak{p}}$ でもあるから，$\Phi_m(X)$ は体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 上の多項式として重根 $\zeta \bmod \mathfrak{p}$ を持つことになる．一方 ζ は $f(X) = X^m - 1$ の根でもある．$f'(X) = mX^{m-1}$ (形式的導関数) だが $p \nmid m$ だから $f(X) \equiv 0 \pmod{\mathfrak{p}}$ は重根を持ち得ない．これは矛盾ゆえ，$G(\zeta^p) \neq 0$. ∥

さて $K = \mathbb{Q}(\zeta)$ を円の m 分体，すなわち $\zeta = \zeta_m$ とする．k を m と素な整数とすると ζ^k は上の定理によって ζ と共役であるから対応 $\zeta \rightsquigarrow \zeta^k$ から $K/\mathbb{Q}$ の自己同型写像が得られる．この自己同型写像を $\sigma(k)$ または σ_k と表す (すなわち $\sigma_k(\zeta) = \sigma(k)(\zeta) = \zeta^k$). $k \equiv 1 \pmod{m}$ ならば $\sigma(k) = e$ (恒等写像) であるから $k \rightsquigarrow \sigma(k)$ から群の準同型写像：$(\mathbb{Z}/(m))^\times \longrightarrow G = G(K/\mathbb{Q})$ が得られる．これは定理 13.1 によって全射であるが，単射でもある ($\because$ $\sigma(k) = \sigma(l)$ より $\zeta^k = \zeta^l$ $\therefore$ $k \equiv l \pmod{m}$). すなわち，

定理 13.2　1 の原始 m 乗根を ζ_m とすると，円の m 分体 $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ のガロア群は $\bmod m$ の既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ と同型である．したがってとくに $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ はアーベル拡大である．

本書の早いうちに勉強した法 m の既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ が新たな意味を持って再登場したのである．代数的整数論を学ぶからには，この定理はまず第一に記憶しておかねばならない．

系　p を奇素数とする．正 p 多角形が作図可能であるためには p が

$$p = 2^{2^n} + 1$$

と表されることが必要十分である．

証明　$\zeta = e^{2\pi i/p} = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$ とすると，複素平面上で $1, \zeta, \zeta^2, \cdots, \zeta^{p-1}$ は正 p 多角形をなしているので，ζ が作図できるかどうかが問題である．$G(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ は位数 $p-1$ の巡回群であるから，ζ が作図可能であるための条件は第10章§1の結果によって $p-1=2^m$ となることである．m が奇素数 ℓ で割れる場合，$m=k\ell$ とすると

$$2^m+1=(2^k)^\ell+1=(2^k+1)((2^k)^{\ell-1}-(2^k)^{\ell-2}+\cdots+1)$$

となって 2^m+1 は素数ではないので $m=2^n$ の形でなければならない．∥

$p=2^{2^n}+1$ という形の素数は**フェルマー素数**と呼ばれている．$n=0$, 1, 2, 3, 4 と置くと

$$3,\ 5,\ 17,\ 257,\ 65537$$

が得られ，これらはどれも素数である．フェルマーはこの先もすべて素数であろうと予想したらしいが，$n=5$ のとき

$$2^{2^5}+1=4294967297=641\times 6700417$$

という因数分解をオイラー (1732年) が発見したという話はよく知られている．この因数分解はやみくもに素数で割っていって見つけたのではなく，フェルマーの小定理を上手に使って見つけるのだが，それについては読者の演習に任せよう．

問題　$2^{2^5}+1=2^{32}+1$ が素数でないとして，その素因数を ℓ としよう．このとき，

1. $2^{64} \equiv 1 \pmod{\ell}$ を示せ．
2. $64|\ell-1$ を論証せよ．
3. $2^{32}+1$ の素因数を見つけよ．

1796年3月30日の朝，起床しようとした刹那，19歳のガウスが正17角形の作図可能性に気付いたという逸話は高木貞治『近世数学史談』によって有名である．ガウスもよほど自慢だったらしく，『整数論』([5]) の中でも

> 円の幾何学的な 3 等分, および 5 等分の可能性はすでにユークリッドの時代に知られていたにもかかわらず, 2000 年という時の流れの中でこの発見に対して何事も付け加えられなかったこと, そうして幾何学者たちのだれもこのような分割と, それから派生する (6 等分, 15 等分といった) 分割以外には幾何学的構成を通じてなしうる分割は存在しない旨を明言していたという事実には驚くべきものがある. (第 365 項)

と自らの仕事の歴史的意義を強調している. 結局, 1 の冪根が開冪で表せることも正 17 角形の作図可能性もガウスによって発見されたのであった. ただし, ガウスは円分体のガロア群の構造 (定理 13.2) などを理論的に把握していた訳ではないので, たとえば $\varphi(n)$ が 5 で割れる場合,「それをより低次の方程式に還元することはできない」と主張しながらも, 証明することはなかった.

ついでに述べると, 5 次以上の代数方程式の不可解性についても円周等分方程式の可解性に関連して次のように述べている：

> 4 次を超える方程式の一般的解法, 言い換えると, 一般的な方程式の 2 項方程式への還元を見いだそうとする卓越した数学者たちの努力はこれまでのところ不首尾に終わってきた. この問題は, 今日の数学の力を超えているというよりは, むしろある不可能な事柄を提示しているのである. それにもかかわらず, このような 2 項方程式への還元を許容する方程式が無数に存在するのも確かである. もしわれわれの円周等分方程式がそのような仲間に数えることが示されたなら, 数学者諸氏のお気に召すであろうことを希望する. (『整数論』第 359 項)

ガウスは方程式論の基本定理の証明を述べた学位論文の中でも「5 次方程式の冪根による解法が不可能であることを厳密に証明するのはさほど難しいことではないであろう」と述べている. その証明を残すことはしなかったに

してもガウスが早くから結果を見通していたことの証拠にはなるであろう.

さて, これもまた円分体論で重要な役割を果たす次の定理が知られている:

定理 13.3 (ディリクレの素数定理)　$(a,m)=1$ とすると初項 a, 公差 m の等差数列 $a+km$ $(k\in\mathbb{N})$ の中には無数に素数が存在する.

この定理は $(\mathbb{Z}/m\mathbb{Z})^\times$ の各類には素数が無数に含まれる, と述べても同じことである. 証明は本書では割愛する. ディリクレというのは整数論に解析学を初めて応用した人で定理 13.3 などが解析数論の濫觴(らんしょう)である.

定理 13.3 は大変な定理であるけれども等差数列が 1 次式だから曲りなりにも証明できるのである. たとえば n^2+1 という形の素数は無数にあるか？といった問題は見てくれからは想像の出来ない, 未だ未解決の大難問である.

ところが一方, 整係数多項式 $f(X_1,\cdots,X_n)$ でその値が素数の全体を尽くすものの存在が不定方程式の解が存在するかどうかを決定するアルゴリズムの問題に関連して近年 J. ロビンスンやマチャセビッチの努力によって見つかった. これは基礎論学者のあげた整数論上の最大の成果であろう.

P を素数全体の集合とすると $X_1\in\mathbb{N},\cdots,X_n\in\mathbb{N}$ に対し $f(X_1,\cdots,X_n)>0$ なる限り $f(X_1,\cdots,X_n)\in P$ であり, 逆に $\forall p\in P$ に対し $\exists X_1\cdots\exists X_n(\in\mathbb{N}); f(X_1,\cdots,X_n)=p$ という性質を持つ多項式 (素数表現多項式) の存在である. 証明された当初は 49 変数の多項式だった. その後 5 変数位まで下がったと聞いているが詳しいことは知らない. ガウスが聞いたら腰を抜かして "Unbelievable! Unthinkable!" と叫ぶに違いない. (もっともどうしてガウスが英語で叫ぶのかは知らないが.)

マチャセビッチによって最終的にヒルベルトの第 10 問題が解決された折に, 副産物として同時に素数表現多項式の構成的存在が確定したのである.

ヒルベルトの第 10 問題というのは, 任意に与えられた整係数不定方程式が整数解を有するや否やを判定する手続き (アルゴリズム) があるか, という問題である. もしそんな手続きが理論上だけでも存在したら大変なことであ

るが，実際はマチャセビッチがJ. ロビンスンなどの成果を基にそんな手続きは存在しないことを証明したのである．不定方程式論は日本ではほやらぬ分野であったからヒルベルトの第 10 問題が否定的に解決されたと聞いても整数論の専門家は大して誰も驚かなかったのだが素数表現多項式の存在にはたまげた (人もいる).

この定理を面白いと思うかどうかは個人差がある．類体論にしたってそうで，たとえば次節以降に述べるヒルベルトの理論を面白いと思う訓練を積んでおかないと「類体論なんてどこが面白いのだろう ?」という小声の批評を洩らす結果を招く．

人によっては証明は「単なる証明」以上のものだ，と考える．証明を知らなければ数学の本当の面白さは理解できないという説である．しかし素数表現多項式の存在に興味を持たない人が証明を一ヵ月かけて読んでみてそれで面白いと思うようになるかというと必ずしもそうではない．私の研究室のゼミで論文を読んだのだが学生諸君はちっとも驚きもしなかったし，おかしがりもしなかった．読者もお気付きのように，この手の数学は普通数学と思われているものとちょっと毛色が変っている．したがって面白いと思う訓練を積んでいないことの方が面白いと思わない主な原因である．私が「数学的真理は人類を超えた，全宇宙的で普遍的な実在である」という説に同意しかねるのは上に述べたような感じ方が根底にあるからである．自分達が信じるものはどんな知的存在にとっても重要なことに違いない，いや，むしろそれに関心を持つかどうかで「知的存在」であるかどうかが判定されるといった考え方ではないかと思うのだが，これは人間中心主義の傲慢であろう．なんとなく，キリスト教と同質の独善がにおって，こうした数学実在主義は私は嫌いである．

言葉における語感のように，仏像における光背の如きものを醸し出す役割を果たすのは数学においても伝統なのである．また，個人的には，どれだけそのために時間を使ったか，なのである．証明を知ることもまたある意味では時間をかけることに意義があるのかもしれない．

It is the time you have wasted for your rose that makes your rose so important.

これは『星の王子さま』という童話の中で，きつねが王子さまに語る言葉で，この本のサワリの部分であろう．初めて私がこの本を読んだときなんともイヤーな気分になった．そのイヤな気分を分析してみるとそのわざとらしい近視眼的な物の見方ということに集約されようか．(日本の童話には子供の素直さと称して近視眼を強調したものが多いが，イギリス，アメリカの童話には大人にも十分楽しめるものがある．)　以来十数年を経て，フランス語はいくらやさしい本でも小説を読むほどには得手でないから，せめて英語で読んでみたら，あのベタベタした感じがしないのではないか，あれはたとえば「王子さま」などという訳語からくる不快感なのではないか，と思いついて英訳本を読んでみたのである．結果は，やっぱり同じことだった．

ただ上に記した言葉は気に入った．私が数学を大切だと思うのは私に才能があるからではもちろんなく，実に下らぬ (そしてけっきょくは何の成果ももたらさなかった) 計算のために延々と費やして来たあの時間のせいなのであって，それ以外の何物のせいでもないのではなかろうか．

雑談が長くなった．最後に，円分体がどうして 2 次体に次いで扱い易い体なのか，その重要な根拠の一つである次の定理を述べておこう：

定理 13.4　ζ を 1 の原始 p 乗根 (p は素数) として，$K = \mathbb{Q}(\zeta)$ とする．このとき $\{1, \zeta, \cdots, \zeta^{p-2}\}$ は K の整数基をなす，すなわち $\mathbb{O}_K = \mathbb{Z}[\zeta]$ である．

証明　任意の $\alpha \in \mathbb{O}_K$ はともかく

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}, \quad a_0, \cdots, a_{p-2} \in \mathbb{Q}$$

と表すことが出来る．$G = G(K/\mathbb{Q})$ として $T_K\alpha = \sum_{\sigma \in G} \alpha^\sigma$ と定義する (α のトレースと呼ばれる)．ζ を一般に 1 の p 乗根 ($\neq 1$) とすれば

$$T_K\zeta = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1$$

であるから

$$T_K\alpha = (p-1)a_0 - a_1 - \cdots - a_{p-2}$$

同様にして，

$$T_K(\zeta\alpha) = -a_0 - a_1 - \cdots - a_{p-2}$$
$$\therefore \quad T_K(1-\zeta)\alpha = pa_0$$

$T_K(\zeta^{-j}\alpha - \zeta\alpha)\ \ (j = 0, 1, \cdots, p-2)$ を同様に計算すると

$$T_K(\zeta^{-j}\alpha - \zeta\alpha) = pa_j$$

を得る．一方，$\zeta^{-j}\alpha - \zeta\alpha \in \mathbb{O}_K$ だから $T_K(\zeta^{-j}\alpha - \zeta\alpha) \in \mathbb{O}_K$.

$$\therefore \quad pa_j = T_K(\zeta^{-j}\alpha - \zeta\alpha) \in \mathbb{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

すなわち pa_j は有理整数である．故に $\alpha \in \mathbb{O}_K \Rightarrow p\alpha \in \mathbb{Z}[\zeta]$.

ところで $\lambda = \zeta - 1$ と置くと

$$\zeta = \lambda + 1, \quad \zeta^2 = \lambda^2 + 2\lambda + 1, \quad \cdots$$

だから $\mathbb{Z}[\lambda] = \mathbb{Z}[\zeta]$ なので

$$p\alpha = b_0 + b_1\lambda + \cdots + b_{p-2}\lambda^{p-2}, \quad b_0, b_1, \cdots, b_{p-2} \in \mathbb{Z} \tag{1}$$

と表せるはずである．一方，

$$N_K\lambda = \prod_{\sigma \in G} \lambda^\sigma = \prod_{j=1}^{p-1}(\zeta^j - 1) = p$$
$$(\because \quad X^{p-1} + \cdots + X + 1 = \prod_{j=1}^{p-1}(X - \zeta^j).\text{これに 1 を代入.})$$

故に $\lambda | p$ だから，(1) を $\bmod\ \lambda$ で考えると

$$b_0 \equiv 0 \pmod{\lambda} \quad \therefore \quad b_0 \in (\lambda) \cap \mathbb{Z} = (p)$$

さらに $\bmod\ \lambda^2$ で考えると

$$b_1\lambda \equiv 0 \pmod{\lambda^2} \quad \therefore \quad b_1 \equiv 0 \pmod{\lambda} \quad \therefore \quad b_1 \equiv 0 \pmod{p}$$

これを続けて $b_j \equiv 0 \pmod{p}\ \ (j = 0, 1, \cdots, p-2)$ を得る．故に $\alpha \in \mathbb{Z}[\lambda] = \mathbb{Z}[\zeta]$ が得られて，証明が終わる． ||

命題　p を奇素数とし，ζ を 1 の原始 p 乗根とすると，

1. $p = \prod_{i=1}^{p-1}(1 - \zeta^i)$
2. 各 i $(1 \leqq i \leqq p-1)$ に対して $(1-\zeta^i)/(1-\zeta)$ は単数である．

証明　1. は上の証明に含まれている．次に

$$\frac{1-\zeta^i}{1-\zeta} = 1+\zeta+\cdots+\zeta^{i-1} \in \mathbb{Z}[\zeta]$$

また ζ^i も 1 の原始 p 乗根だから $\dfrac{1-\zeta}{1-\zeta^i} \in \mathbb{Z}[\zeta]$ となり，2. を得る．‖

$\pi = 1-\zeta$ と置けば，上の命題により

$$p = \varepsilon\pi^{p-1} \quad (\varepsilon \in U_K)$$

と書けることになる (U_K は K の単数群)．イデアルで考えれば

$$(p) = (\pi)^{p-1} \tag{2}$$

一般に

$$(p) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}, \quad \sum_{i=1}^{g} e_i f_i = p-1$$

と分解するはずなので，(2) は (π) が素イデアル (すなわち π は素元) で，$e = p-1$, $f=1$, $g=1$ であることを示している．一般に相対代数体 L/K で，ある素イデアル $\mathfrak{p}$ が次数一杯に分岐しているとき，すなわち

$$\mathfrak{p} = \mathfrak{P}^{[L:K]}$$

となるとき，$\mathfrak{P}$(あるいは $\mathfrak{p}$) は L/K で**完全分岐**していると言うのだが，この用語を使えば次の系が得られる：

命題の系　1 の p 分体において p は完全分岐する．

定理 13.5　1 の p 分体 K の判別式 D_K は次で与えられる：

$$D_K = (-1)^{\frac{p-1}{2}} p^{p-2}$$

証明　ζ の満たす既約多項式を $f(X)$ とすると，判別定理 (定理 11.11) の証明で述べたように，$\mathbb{O}_K = \mathbb{Z}[\zeta]$ の場合，$D_K = (-1)^{\frac{p-1}{2}} N_K f'(\zeta)$ が成り立つ．$f(X) = (X^p-1)/(X-1)$ だから

$$f'(X) = \frac{pX^{p-1}(X-1)-(X^p-1)}{(X-1)^2} \quad \therefore \quad f'(\zeta) = \frac{p\zeta^{-1}}{\zeta - 1}$$

$$\therefore \quad D_K = (-1)^{\frac{p-1}{2}} \prod_{j=1}^{p-1} \frac{p\zeta^{-j}}{\zeta^j - 1} = p^{p-1}(-1)^{\frac{p-1}{2}} \prod_{j=1}^{p-1} (1-\zeta^j)^{-1}$$

$$= (-1)^{\frac{p-1}{2}} p^{p-2} \quad \|$$

§ 2. 有限体論

F を有限体とする．F の標数を p とすれば，$F \supseteqq \mathbb{F}_p (\simeq \mathbb{Z}/p\mathbb{Z})$ である．F を $\mathbb{F}_p$ 上のベクトル空間と見たときの次元を $f(=[F:\mathbb{F}_p])$ とし，基底を $\omega_1, \cdots, \omega_f$ とすれば，F の元はすべて

$$a_1\omega_1 + \cdots + a_f\omega_f \quad (a_1, \cdots, a_f \in \mathbb{F}_p)$$

という形に唯一通りに書けるから，$|F| = p^f$ である．

定義　$|F| = q = p^f$ なる体を q 元体という．

$F^\times = F - \{0\}$ は位数 $q-1$ の巡回群をなすのであった (定理 8.2 系)．故に次の定理は自明である：

定理 13.6　有限体 K の位数を $q = p^f$ とすると，K の元はすべて方程式

$$X^q - X = 0 \tag{3}$$

の根である．

因数定理 (p.50 の問題) によって体の中で q 次方程式は q 個以内しか解を持ち得ないから，(3) は K の元以外に解を持たない．

気分をすっきりさせるためには $\mathbb{F}_p$ の代数的閉包 $\overline{\mathbb{F}_p}$ を一つ固定しておいて，すべての考察を $\overline{\mathbb{F}_p}$ の中でやることにするのが良い．このとき

$$K = \{x(\in \overline{\mathbb{F}_p}) \mid x^q - x = 0\} \tag{4}$$

である．

定理 13.7　p を素数とする．$q = p^f$ を任意に与えるとき，q 元体が ($\overline{\mathbb{F}_p}$ の中に) 一つだけ存在する．

証明　(4) とすれば，K はちょうど q 個の元からなる．($\because$ $X^q - X$ という多項式の形式的微分は $qX^{q-1} - 1 = -1$ ($\because$ $p|q$) だから，$X^q - X$ と互いに素であって，$X^q - X = 0$ は重複根を持たない．)

次に $x, y \in K$ に対して

$$(x+y)^q = x^q + y^q = x + y$$
$$(xy)^q = x^q y^q = xy$$

($i = 1, \cdots, p-1$ のとき ${}_pC_i \equiv 0 \pmod p$ だからである．)　故に $x + y \in K$, $xy \in K$ となり，K は体をなす．これで存在が示せた．次に F を q 元体 (もちろん $F \subseteqq \overline{\mathbb{F}_p}$ とする) とすれば，$x^q = x$　$(\forall x \in F)$ だから $F \subseteqq K$　$\therefore$ $F = K$．∥

次々と単純で美しい定理が証明されてきたが，次が最後で，しかも極め付きである：

定理 13.8　L/K を標数 p の有限体の拡大体とし，$|K| = q, |L| = q^f$ とする．このとき L/K はガロア拡大であって，そのガロア群 $G(L/K)$ は f 次巡回群である．

証明　$\varphi : L \longrightarrow \overline{\mathbb{F}_p}$ を $\varphi(x) = x^q$ によって定義する．φ が単射準同型であることは $(x+y)^q = x^q + y^q, (xy)^q = x^q y^q$ によって明らかである．$\varphi(L) \subseteqq L$ だが，単射性によって $\varphi(L) = L$ が成り立つ (有限集合の原理)．したがって φ は L の自己同型写像であるが，$x \in K$ ならば $x^q = x$ なので $\varphi(x) = x$　$(\forall x \in K)$ となり，φ は L/K の自己同型写像であることになる．

次に $0 \leqq i < j < f$ ならば $\varphi^i \neq \varphi^j$ であることを示す．α を巡回群 $L^\times$ の生成元とすると

$$\varphi^i(\alpha) = \alpha^{q^i}, \quad \varphi^j(\alpha) = \alpha^{q^j}$$

で $\alpha^{q^i} \neq \alpha^{q^j}$ が成り立つ．($\because$ $L = \{\alpha^\nu \mid \nu = 0, 1, \cdots, q^f - 1\}$)　故に $\varphi^i \neq \varphi^j (0 \leqq i < j < f)$ である．$\varphi^0(= e), \varphi^1, \cdots, \varphi^{f-1}$ は相異なる $f = [L : K]$ 個の自己同型写像である．故に L/K はガロア拡大であって，

$$G(L/K) = \{\varphi^0, \varphi^1, \cdots, \varphi^{f-1}\}$$

となり，f 次巡回群である．‖

[注意]　有限体論にガロアの理論がそのまま適用できることを見ておかねばならない．第 12 章を見直してみると，$f(X) = 0$ が K 上の既約方程式ならば $\overline{K}$ (これは $\overline{\mathbb{F}_p}$ と一致する) において $\deg f$ 個の相異なる根を持つことが成り立ちさえすれば，相対拡大 L/K の共役写像が $[L : K]$ 個あることになって，他はすべて何の支障もなく理論が展開できることがわかる．

そこで，$f(X)$ を有限体 K 上の既約多項式としよう．$f(X) = 0$ が重根を持ち得るのは形式的微分 $f'(X)$ が恒等的に 0 となる場合である ($\because$ $f' = 0$ でないなら $\deg f' < \deg f$ となって，公約因子を持ち得ないからである)．$f'(X) = 0$ となるのは，K 上の多項式 $g(X)$ があって $f(X) = g(X^p)$ と書ける場合である．

今 K の自己同型写像 $\psi(x) = x^p$ を考えてみよう．これが全射であるから，各 $a \in K$ は $a = a^{*p}$　$(a^* \in K)$ と表せる．

$$\begin{aligned} g(X^p) &= a_0 + a_1 X^p + \cdots + a_n X^{np} \quad (a_i \in K) \\ &= a_0^{*p} + a_1^{*p} X^p + \cdots + a_n^{*p} X^{np} \quad (a_i^* \in K) \\ &= (a_0^* + a_1^* X + \cdots + a_n^* X^n)^p \end{aligned}$$

故に，$g(X^p)$，すなわち $f(X)$，は K で既約ではないことになり，仮定に反する．つまり，K 上の既約方程式は重根を持たないのである．これによって有限体論にガロアの理論が適用できることがわかった．

§ 3.　フロベニウス写像

有限体論を代数体の研究に応用する．

L/K を相対代数体，$\mathfrak{P}$ を L の素イデアル，そして $\mathfrak{p} = \mathfrak{P} \cap \mathbb{O}_K$ としよう．$\mathfrak{p}$ は K の素イデアルであった．さらに $\mathbb{O}_L/\mathfrak{P}$ を ℓ，$\mathbb{O}_K/\mathfrak{p}$ を k と記せば ℓ, k

は有限体で $\ell \supseteqq k$ と考えられるのであった．すなわち $k = \{\alpha \bmod \mathfrak{P} \mid \alpha \in \mathbb{O}_K\}$ と考えれば $k \subseteqq \ell$ となる．

いま L/K が特にガロア拡大であると仮定しよう．$\sigma \in G = G(L/K)$ が $\sigma\mathfrak{P} = \mathfrak{P}$ (つまり，$x \in \mathfrak{P} \Longrightarrow \sigma x \in \mathfrak{P}$) を満足するならば $\overline{x} \in \ell$ に対して

$$\overline{\sigma x} = \overline{\sigma x}$$

と定義することによって，σ から $\ell = \mathbb{O}_L/\mathfrak{P}$ の自己同型写像 $\overline{\sigma}$ が誘導されることになる．($x \equiv y \pmod{\mathfrak{P}}$ ならば $\sigma x \equiv \sigma y \pmod{\mathfrak{P}}$ となり $\overline{\sigma}$ は well defined となるのである．)

定義　$Z = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ と置いて，Z を $\mathfrak{P}$ の**分解群**，そして Z の固定 体 L^Z を $\mathfrak{P}$ の**分解体**と呼ぶ．

Z が G の部分群であることはすぐにわかることだから，自分で証明をやってみること．

上述のことから

$$\varphi(\sigma)(\overline{x}) = \overline{\sigma(x)} \quad (\sigma \in Z)$$

と定義すると準同型写像 $\varphi : Z \longrightarrow G(\ell/k)$ が定義される．φ の核を T と記すと

$$\begin{aligned} T &= \{\sigma(\in Z) \mid \overline{\sigma x} = \overline{x} \quad (\forall x \in \mathbb{O}_L)\} \\ &= \{\sigma(\in Z) \mid x^\sigma \equiv x \pmod{\mathfrak{P}}\ (\forall x \in \mathbb{O}_L)\} \end{aligned}$$

つまり $\ell = \mathbb{O}_L/\mathfrak{P}$ の恒等自己同型を誘導するようなものの集まりが T である．この T を $\mathfrak{P}$ の**惰性群**と言い，T の固定体 L^T を $\mathfrak{P}$ の**惰性体**と言う．群の準同型定理から単射 $\overline{\varphi} : \mathbb{Z}/T \longrightarrow \overline{G} = G(\ell/k)$ が与えられたことになるが，次節で証明するように，この $\overline{\varphi}$ は実は全射でもある：

定理 13.9　$Z/T \simeq G(\ell/k)$．特に，T は Z の正規部分群，Z/T は巡回群であり，$(Z : T) = [\ell : k]$ が成り立つ．

こういう見事な定理が成り立つので前節で有限体論をやった甲斐があるというものだ．定理 13.9 を前提とすれば，$G(\ell/k)$ の生成元 ψ は $\psi(x) = x^q$ $(q = |k|)$ で与えられたから，

$$\sigma(x) \equiv x^q \pmod{\mathfrak{P}}$$

を満たす $\sigma(\in Z)$ が少なくとも一つ存在することになる．こういう σ を L/K における $\mathfrak{P}$ の**フロベニウス写像**と呼んでいる．元々はフロベニウス置換と呼ばれて来たのだが，ちょっと代数学の用語とそぐわなくなってきたので，本書では「写像」と言うことにする．なお $|T| = 1$ のときはフロベニウス写像は唯一つに定まることに注意しよう．

§4. ヒルベルトの理論

L/K を相対代数体とする．$\mathfrak{p}$ を K の素イデアルとする．$\mathfrak{p}\mathbb{O}_L$ を簡単のため $\mathfrak{p}$ と書くのだが，$\mathfrak{p}$ は L において

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \tag{5}$$

というように相異なる素イデアルの冪積に分解される．各 $\mathfrak{P}_j$ を $\mathfrak{p}$ の**素因子**と呼ぶことにしよう．次の定理は第 11 章 §5 の式 (8) の拡張である：

定理 13.10　$f_j = [\mathbb{O}_L/\mathfrak{P}_j : \mathbb{O}_K/\mathfrak{p}]$ (相対次数) と置けば，

$$e_1 f_1 + \cdots + e_g f_g = [L : K]. \tag{6}$$

(5) の両辺のノルムを取ると，

$$N_L\mathfrak{p} = \prod_{j=1}^{g} (N_L\mathfrak{P}_j)^{e_j} = \prod_{j=1}^{g} (N_K\mathfrak{p})^{e_j f_j}$$

が得られるから，証明は次の補題に帰着される：

補題　L の素イデアル $\mathfrak{P}$ に対して $\mathfrak{P} \cap K = \mathfrak{p}$，また $f = [\mathbb{O}_L/\mathfrak{P} : \mathbb{O}_K/\mathfrak{p}]$ とすると，次が成り立つ：

$$N_L\mathfrak{p} = (N_K\mathfrak{p})^{[L:K]}$$

証明　$\mathbb{Z}\cap\mathfrak{p}=(p)$ として，次のような $\alpha\in\mathbb{O}_K$ を選ぶことができる：

$$(\alpha)=\mathfrak{p}\mathfrak{a},\quad (\mathfrak{a},\ (p))=1$$

選び方：K において $(p)=\mathfrak{p}^s\mathfrak{b}$, $(\mathfrak{p},\ \mathfrak{b})=1$ と分解する．π を $\mathfrak{p}$ の元だが，$\mathfrak{p}^2$ の元ではない ($\mathbb{O}_K$ の) 元とする．$\alpha\equiv\pi(\mathrm{mod}\ \mathfrak{p}^2)$, $\alpha\equiv 1\ (\mathrm{mod}\ \mathfrak{b})$ なる数の存在は孫子の定理 (CRT) によって保証されている．$(\alpha)=\mathfrak{p}\mathfrak{a}$ と因数分解すると，α の選び方から $((p),\ \mathfrak{a})=1$ である．

$$N_L\mathfrak{p}N_L\mathfrak{a}=N_L(\alpha)=|N_L\alpha|=|N_K\alpha|^n=(N_K(\alpha))^n=(N_K\mathfrak{p})^n(N_K\mathfrak{a})^n$$

(ここに定理 11.7 を二度使った．また $n=[L:K]$ とする.)　ところで $(N_K\mathfrak{p},\ N_K\mathfrak{a})=1$, $(N_L\mathfrak{p},\ N_L\mathfrak{a})=1$ だから結果を得る． ∥

なお，ノルムの意味を考えれば，補題は $\mathbb{O}_L/\mathfrak{p}\mathbb{O}_L$ が体 $\mathbb{O}_K/\mathfrak{p}$ 上の $[L:K]$ 次元ベクトル空間であるということを意味していることを注意しておこう．

(5) や (6) という関係は L/K がガロア拡大の場合にはもっと整然とした形を取る：

定理 13.11　1. L/K を n 次ガロア拡大とし，そのガロア群を G と記す．K の素イデアル $\mathfrak{p}$ の L における素因子の一つを $\mathfrak{P}$ とすれば，任意の $\sigma(\in G)$ に対して $\mathfrak{P}^\sigma(=\sigma\mathfrak{P})=\{\sigma x\mid x\in\mathfrak{P}\}$ は $\mathfrak{p}$ の素因子である．また任意の素因子は $\mathfrak{P}^\sigma$ の形に表せる．

2. $\mathfrak{p}$ の相異なる素因子を $\mathfrak{P}_1,\cdots,\mathfrak{P}_g$ とすれば $e_1=\cdots=e_g(=e)$, $f_1=\cdots=f_g(=f)$ が成り立つ．したがって $\mathfrak{p}$ の L での分解は

$$\mathfrak{p}=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$$

の形となり，$efg=n$ が成り立つ．

証明　$\mathfrak{P}$ を $\mathfrak{p}$ の素因子とすれば (5) から

$$\mathfrak{p}=\mathfrak{P}\mathfrak{A}$$

という L のイデアル $\mathfrak{A}$ が存在する．両辺に σ をほどこせば

$$\mathfrak{p}=\mathfrak{p}^\sigma=\mathfrak{P}^\sigma\mathfrak{A}^\sigma$$

となり，$\mathfrak{P}^\sigma$ も $\mathfrak{p}$ の素因子である．次に $\mathfrak{Q}$ (ドイツ文字の Q) が $\mathfrak{p}$ の一つの素因子であるとして，どの $\sigma(\in G)$ に対しても $\mathfrak{Q} \neq \mathfrak{P}^\sigma$ としよう．連立合同式

$$x \equiv 0 \pmod{\mathfrak{Q}}, \quad x \equiv 1 \pmod{\mathfrak{P}^\sigma} \quad (\forall \sigma \in G)$$

は孫子の定理 (CRT) によって解 $x = \alpha$ を $\mathbb{O}_L$ に持つ．$a = \prod_{\sigma \in G} \alpha^\sigma$ と置くと $\alpha \in \mathfrak{Q}$ によって $a \in \mathfrak{Q}$，また a は $a^\sigma = a$ $(\forall \sigma \in G)$ を満たすから $a \in \mathbb{O}_K$ も言える．$\therefore\ a \in \mathfrak{Q} \cap \mathbb{O}_K$．ところが $\mathfrak{Q} \cap \mathbb{O}_K = \mathfrak{p}$ だから $a \in \mathfrak{p}$，また $\mathfrak{p} \subseteqq \mathfrak{P}$ だから $\prod_{\sigma \in G} \alpha^\sigma \in \mathfrak{P}$．$\mathfrak{P}$ は素イデアルだから $\exists \sigma(\in G)$; $\alpha^\sigma \in \mathfrak{P}$．この σ に対して $\alpha \in \mathfrak{P}^{\sigma^{-1}}$．これは $\alpha \equiv 0 \pmod{\mathfrak{P}^{\sigma^{-1}}}$ を意味するが $\alpha \equiv 1 \pmod{\mathfrak{P}^\sigma}$ が任意の σ に対して成立するはずだから矛盾．故に $\mathfrak{P}^\sigma$ は $\mathfrak{p}$ の素因子の全体をわたることが証明された．

$\mathfrak{p}$ の素因子 $\mathfrak{P}$ を一つ固定する．$\mathfrak{P}$ の分解群を Z とする．

$$\sigma \in Z \Longleftrightarrow \mathfrak{P}^\sigma = \mathfrak{P}$$

だったから G の Z による類別 G/Z の代表系を $\{\sigma_1, \cdots, \sigma_g\}$(ただし $\sigma_1 = e$(単位元)) とすれば $\{\mathfrak{P}^{\sigma_1}, \cdots, \mathfrak{P}^{\sigma_g}\}$ がちょうど $\mathfrak{p}$ の素因子の全体となっていることがわかる．($\sigma\mathfrak{P} \equiv \tau\mathfrak{P} \Longleftrightarrow \tau^{-1}\sigma\mathfrak{P} = \mathfrak{P} \Longleftrightarrow \sigma \in \tau Z$ による．$\mathfrak{P}^\sigma = \sigma\mathfrak{P}$ に注意．) $\mathfrak{P}^{\sigma_j} = \mathfrak{P}_j$ と置く ($\mathfrak{P}_1 = \mathfrak{P}$)．

σ_j を σ と書いて固定する．写像 $\varphi : \mathbb{O}_L \longrightarrow \ell_j$ $(= \mathbb{O}_L/\mathfrak{P}_j)$ を $\varphi(x) = x^\sigma \pmod{\mathfrak{P}_j}$ で定義すれば φ は環の準同型写像で，その核は $\{x \in \mathbb{O}_L \mid x^\sigma \in \mathfrak{P}_j\} = \{x \in \mathbb{O}_L \mid x \in \mathfrak{P}\} = \mathfrak{P}$ だから $\mathbb{O}_L/\mathfrak{P} \simeq \mathbb{O}_L/\mathfrak{P}_j$．故に ℓ_j はすべて同型．したがって $f_1 = \cdots = f_g$ が成り立つ．次に

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

の両辺に σ_j を作用させれば

$$\mathfrak{p} = (\mathfrak{P}_1^{\sigma_j})^{e_1} \cdots (\mathfrak{P}_g^{\sigma_j})^{e_g} = \mathfrak{P}_j^{e_1} \cdots$$

となり素イデアル分解の一意性から $e_j = e_1$．$\therefore\ e_1 = \cdots = e_g$．‖

定理の証明から次の系を得る．

系　L の素イデアル $\mathfrak{P}$ の L/K における分解群を Z とすると $|Z| = ef$.

定理 13.12　L/K を n 次相対代数体とし，$\mathfrak{P}$ を L の素イデアル，$\mathfrak{p} = \mathfrak{P} \cap K$, $f = [\mathbb{O}_L/\mathfrak{P} : \mathbb{O}_K/\mathfrak{p}]$ とする．

$$N_{L/K}\mathfrak{P} = \mathfrak{p}^f \quad \textbf{(相対ノルム)}$$

と定義すると，

$$N_{L/K}\mathfrak{P} = \prod_{j=1}^{n} \mathfrak{P}^{(j)}$$

が成り立つ．ここに (j) $(j = 1, \cdots, n)$ は L/K の共役写像を表す．

証明　1. L/K がガロア拡大の場合

ガロア群を G とし，Z を $\mathfrak{P}$ の分解群する．G の Z による類別の代表系を $\{\sigma_1, \cdots, \sigma_g\}$ とすると，定理 13.11 の系によって

$$\prod_{\sigma\in G} \mathfrak{P}^{\sigma} = \prod_{j=1}^{g} (\prod_{\sigma\in Z} \mathfrak{P}^{z})^{\sigma_j} = (\prod_{j=1}^{g} \mathfrak{P}^{\sigma_j})^{ef} = \mathfrak{p}^f$$

2. 一般の場合

$K \subsetneqq L \subsetneqq F$ なる K 上のガロア拡大 F を取る．また $\mathfrak{P}$ の F における素因子を一つ取って $\mathfrak{P}_F$ とする．以下の計算で $f(L/K)$ 等は相対次数を表すものとする．G, H をそれぞれ F/K, F/L のガロア群とすると，

$$N_{F/K}\mathfrak{P}_F = \prod_{\sigma\in G} \mathfrak{P}_F^{\sigma} = \prod_{j=1}^{n} (\prod_{\tau\in H} \mathfrak{P}_F^{\tau})^{(j)} = \prod_{j=1}^{n} (\mathfrak{P}^{f(F/L)})^{(j)}$$

また一方では，

$$N_{F/K}\mathfrak{P}_F = \mathfrak{p}^{f(F/K)}$$

だが，相対次数の定義によって $f(F/K) = f(F/L)f(L/K)$ が成り立つから，一般の場合の証明も終わる．∥

この定理によって数のノルムとイデアルのノルムの関係が明らかになった．

定理 13.13　L/K が代数体のガロア拡大で $\mathfrak{P}$ が L の素イデアルのとき，$\mathfrak{P}$ の分解群，惰性群を Z, T とし，$\mathfrak{P}$ の分岐指数を e，相対次数を f とすれば

$$|T| = e, \quad (Z : T) = f.$$

また Z/T は f 次の巡回群である．

証明　G を L/K のガロア群とする．また Z の固定体，すなわち分解体 L^Z を M とする．$\mathfrak{P} \cap \mathbb{O}_M = \mathfrak{q}$ とおき，剰余類体 $\mathbb{O}_M/\mathfrak{q}$ を m と書く．また今まで通り，$\ell = \mathbb{O}_L/\mathfrak{P}$, $k = \mathbb{O}_K/\mathfrak{p}$ である．L/M における $\mathfrak{P}$ の分岐指数を e'，相対次数を f' として定理 13.11 とその系を適用すれば，いまは L/M のガロア群自身が分解群となっているから

$$[L : M] = e'f'$$

である．$f' = [\ell : m] \leqq [\ell : k] = f$，また $\mathfrak{p} = \mathfrak{q}^{e''} \cdots$ (in M), $\mathfrak{q} = \mathfrak{P}^{e'} \cdots$ (in L) とすると $e = e'e''$ だから，やはり $e' \leqq e$.

一方，定理 13.11 の系より $[L : M] = ef$ だから $e' = e, f' = f$ を得る．

次に $\rho \bmod \mathfrak{P}$ を乗法群 $(\mathbb{O}_L/\mathfrak{P})^\times$ の生成元とする．

$$F(X) = \prod_{z \in Z} (X - \rho^z), \qquad G(X) = \prod_{i=0}^{f-1} (X - \rho^{q^i})$$

(ここに $q = |k| = |m|$) と置くと，どちらも $\bmod \mathfrak{P}$ では $m[X]$ に属する．$G(X) \bmod \mathfrak{q}$ は既約だから，$\mathfrak{q}$ を法として，$G|F$ である．故に，$\exists z \in Z[\rho^z \equiv \rho^q \pmod{\mathfrak{P}}]$ となり，定理の証明が終わる．‖

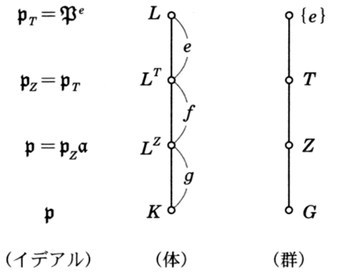
なお，この結果，定理 13.9 の証明も終わったことになる．

次がヒルベルトの理論の主要部である：

定理 13.14　$L/K, \mathfrak{P}$ などはこれまでと同じとする．$\mathfrak{P}$ の分解体を L^Z，惰性体を L^T とし，$\mathfrak{P} \cap \mathbb{O}_{L^Z} = \mathfrak{p}_Z$, $\mathfrak{P} \cap \mathbb{O}_{L^T} = \mathfrak{p}_T$．また $e(L/K)$ 等でもって $\mathfrak{P}$ の L/K における分岐指数等を表すことにすると，

1. $\mathfrak{p}_T = \mathfrak{P}^e$, $e = e(L/K) = e(L/L^T)$, $f(L/L^T) = 1$,
2. $\mathfrak{p}_Z = \mathfrak{p}_T$, $e(L^T/L^Z) = 1$, $f(L^T/L^Z) = f(L/K) = f$

が成り立つ．つまり分岐は L/L^T でしか起らず，剰余類体の変化は L^T/L^Z でしか起らない．$\mathfrak{p}_Z$ は L^T で考えても素イデアルのままである．



なぜ L^Z が分解体，L^T が惰性体と呼ばれるか，この定理によってわかる．惰性とは，素イデアルのまま変化なく移行する，の心であろう．なお T は Trägheitsgruppe，Z は Zerlegungsgruppe というドイツ語の頭文字である．ヒルベルトはドイツ人であるし，当時は数学，特に整数論はドイツが中心だったから，ドイツ語が使われるのは当然である．集合論では，ヘブライ語の字母 ℵ(アレフ) も使われることでもあるし，「甲，乙」や「い，ろ，は」などが数学記号として世界的に使われるのを見たいものだ．

証明　(**定理** 13.14 **の証明**)　定理 13.13 からほぼ直ちに出る．たとえば 1. を示そう．$\mathfrak{P}$ の L/L^T に関する惰性群は定義により T で，それは $G(L/L^T)$ である．定理 13.13 によって $|T| = e$，かつ $f(L/L^T) = 1$ である．∥

問題　2. を示せ．

[ヒント]　1. から $\mathfrak{p}_T$ は L^T/L^Z において不分岐である．

これで定理 13.14 の証明は終わったものとする．

惰性群をさらに分岐群という部分群の列に分けるところまで精緻に考察するのがヒルベルト理論の全貌なのだが，そこまでは扱わない．そこまでやる必要性を感じないので，「割愛する」とは言わないでおこう．

第14章　類体論概説

§1. 円分体の場合

有理数体上の円分体は類体論のひな型である．ζ_m を1の原始 m 乗根とすると $K=\mathbb{Q}(\zeta_m)$ のとき，$G(K/\mathbb{Q})\simeq(\mathbb{Z}/m\mathbb{Z})^\times$ で，これはアーベル群である．また $\mathbb{O}_K=\mathbb{Z}[\zeta_m]$ であるといった事実によって，円分体では実にキレイな形で素数の分岐・分解が決定できる．しかし，あまりに1の冪根であるという特殊性に依存していることから，これをそのまま一般の代数体上のアーベル拡大の理論に一般化できることを予感させるものは何もなかった．かえって，類体論が完成して初めて，円分体は $\mathbb{Q}$ 上の類体であることが認識されるのである．

$m=\ell_1^{n_1}\cdots\ell_s^{n_s}$ を m の素因数分解とするとき $\zeta_{\ell_1^{n_1}}\cdots\zeta_{\ell_s^{n_s}}$ が1の原始 m 乗根となることによって

$$\mathbb{Q}(\zeta_m)=\mathbb{Q}(\zeta_{\ell_1^{n_1}})\cdots\mathbb{Q}(\zeta_{\ell_s^{n_s}})$$

は明らかである．これによって円分体における分岐・分解に関する命題は大抵 $\mathbb{Q}(\zeta_{\ell^n})$ の場合に還元される．また $\mathbb{Q}(\zeta_{\ell^n})$ における命題は $\mathbb{Q}(\zeta_\ell)$ の場合とほぼ同一の方法で証明される．一般の場合の証明は現れる指数の計算が複雑になったり，場合分けが増えたりして，見通しを悪くし，本質を見えなくするだけだから，命題は一般の場合で表明するが，証明は $\mathbb{Q}(\zeta_\ell)$ の場合に限定することにする．これによって本質的に失われるものはほとんどない．

$\zeta = \zeta_m$ を 1 の原始 m 乗根とし，$K = \mathbb{Q}(\zeta)$ とする．このとき $G(K/\mathbb{Q})$ は $(\mathbb{Z}/m\mathbb{Z})^\times$ と同型で，その同型対応 σ は $(a,m) = 1$ なる a に対して $\sigma(a)$: $\zeta \rightsquigarrow \zeta^a$ によって与えられるのだった．特に m を割らない素数 p に対しては $\sigma(p)$ は p の上にある K の素イデアル $\mathfrak{p}$ のフロベニウス写像になっている，というのが円分体の相互法則の内容である：

定理 14.1 (円分体の相互法則)　K を円の m 分体とする．$p \nmid m$ なる素数 p について，$\mathfrak{p}$ を p の上にある素因子とする：$\mathfrak{p} \cap \mathbb{Z} = (p)$．このとき $\zeta^\sigma = \zeta^p$ によって定まる $\sigma = \sigma(p) \in G(K/\mathbb{Q})$ は $\mathfrak{p}$ のフロベニウス写像である．

証明　先述のように $m = \ell$ (素数) の場合を扱う．素数 p $(\neq \ell)$ の上にある素因子の一つを $\mathfrak{p}$ と書くと，そのフロベニウス写像 σ は

$$\alpha^\sigma \equiv \alpha^p \pmod{\mathfrak{p}}$$

で与えられるのであった．$\mathbb{O}_K = \mathbb{Z}[\zeta]$ (ここに$\zeta = \zeta_\ell$) だから $\alpha = \zeta$ に対して上の合同式が成り立てば十分である：

$$\zeta^\sigma \equiv \zeta^p \pmod{\mathfrak{p}}$$

$\zeta^\sigma = \zeta^a$ となる a が存在するから，

$$\zeta^a \equiv \zeta^p \pmod{\mathfrak{p}}$$

$$\therefore \quad \zeta^p(1 - \zeta^{a-p}) \in \mathfrak{p}$$

ζ は単数だから

$$1 - \zeta^{a-p} \in \mathfrak{p} \tag{1}$$

を得る．$a \not\equiv p \pmod{\ell}$ ならば ζ^{a-p} は 1 の原始 ℓ 乗根である．このとき，$(\ell) = (1-\zeta)^{\ell-1}$ であり，$1-\zeta$ は ℓ の唯一つの素因子だったから，(1) は起り得ない ($\ell \neq p$ に注意)．$\therefore$ $a \equiv p \pmod{\ell}$．故に $\zeta^\sigma = \zeta^p$ である．∎

(p)の上にある素イデアルはそのうちの一つを$\mathfrak{p}$とすると$\mathfrak{p}^\sigma(\sigma \in G(K/\mathbb{Q}))$と表せる．円分体の場合は $G(K/\mathbb{Q})$ がアーベル群なので，いずれの $\mathfrak{p}^\sigma$ についても，そのフロベニウス写像は同一である．

$$(\because)\ \ \alpha^{\tau} \equiv \alpha^{p} \pmod{\mathfrak{p}} \Longleftrightarrow (\alpha^{\sigma})^{\tau} \equiv (\alpha^{\sigma})^{p} \pmod{\mathfrak{p}^{\sigma}}$$
$$\Longleftrightarrow \alpha^{\tau} \equiv \alpha^{p} \pmod{\mathfrak{p}^{\sigma}} \quad (\forall \alpha \in \mathbb{O}_K)$$

したがって $\mathfrak{p}$ のフロベニウス写像と言わずに，p のフロベニウス写像と言うことにする．

m の素因子だけが $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ で分岐することは $m=\ell$ の場合既に示してあるが，一般の場合はすぐ後で説明する．これを前提として次が示される：

系 1 (**分解定理**)　p を自然数 m を割らない素数とする．

$$p^{f} \equiv 1 \pmod{m}$$

を満たす最小の自然数 f を取ると p は円の m 分体 K において

$$(p)=\mathfrak{p}_1\cdots\mathfrak{p}_g, \quad N_K\mathfrak{p}_j = p^{f} \qquad (j=1,\cdots,g)$$

と g 個 $(g=\varphi(m)/f)$ の素因子に分解される．

証明　$p \nmid m$ より p は $K/\mathbb{Q}$ で不分岐である．$N_K\mathfrak{p}_j = p^{f_0}$ とすると f_0 は分解群 Z の位数，すなわち p のフロベニウス写像 $\sigma(p)$ の位数であった (定理 13.9)．つまり f_0 は

$$\sigma(p)^{f_0} = e \ \ (\text{恒等写像})$$

となる最小の自然数である．定理 14.1 によって $\zeta^{\sigma(p)^{f_0}} = \zeta^{p^{f_0}} = \zeta$ だから，f_0 は $p^{f_0} \equiv 1 \pmod{m}$ を満たす最小の数．$\therefore\ f_0 = f$　‖

円分体の場合はこれで終わりだが，円分体の部分体の場合も導いておこう．

系 2　K を円の m 分体の部分体とし，K にガロアの意味で対応する $(\mathbb{Z}/m\mathbb{Z})^{\times}$ の部分群を H とする：

$$H = \{a \bmod m \mid x^{\sigma(a)} = x \ \ (\forall x \in K)\}$$

ここに σ は $\zeta^{\sigma(a)} = \sigma^{a}$ で定められる $G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ の元である．このとき，つぎが成り立つ：

(1) $G(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^{\times}/H$,

しかも，p が m を割らない素数のときは，この同型対応による p の類の像は K における p のフロベニウス写像になっている．

(2) p を $p \nmid m$ なる素数とする．$p^f \bmod m \in H$ なる最小の自然数 f を選ぶと p は K において

$$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g, \quad N_K \mathfrak{p}_j = p^f \qquad (j = 1, \cdots, g)$$

と $g = \dfrac{1}{f}[K : \mathbb{Q}]$ 個の素イデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ の積に分解される．

(3) K を含む最小の円分体が m 分体である場合 (すなわち，m が最小に取ってある場合) は (p) が $K/\mathbb{Q}$ で分岐する必要十分条件は $p|m$ なることである．

次の問題を参考にすれば (3) 以外の証明は易しい：

問題　$K \subsetneqq M \subsetneqq L$ とし，$L/K, M/K$ はともにガロア拡大であるとする．$\mathfrak{P}$ を L/K で不分岐な L の素イデアル，また $\mathfrak{p}_M = \mathfrak{P} \cap M$ と置く．τ を $\mathfrak{P}$ の L/K におけるフロベニウス写像とすれば $\tau|M$(τ の M への制限) は $\mathfrak{p}_M$ の M/K におけるフロベニウス写像である．このことを示せ．

[ヒント]　フロベニウス写像の定義による．

円分体の部分体における素数の分解の様子が基礎体 $\mathbb{Q}$ における群 ($(\mathbb{Z}/m\mathbb{Z})^\times$ の商群) の情報で決定される，そもそもガロア群自身が基礎体で表現された群と同型である，というのが類体論のひな型たるゆえんである．

なお，有理数体上のアーベル拡大は実はある円分体の部分体である (**クロネッカー–ヴェーバーの定理**)．したがって事はさらに単純明快である．類体論との比較で言えば，類体が円分体とその部分体にあたり，「すべてのアーベル拡大は類体である」という「逆定理」がクロネッカー–ヴェーバーの定理にあたる．したがってクロネッカー–ヴェーバーの定理は類体論の結果として導くことができる．

最後に，円分体 $\mathbb{Q}(\zeta_m)$ で分岐するイデアルは m の素因数に限ることを見ておこう．

定理 14.2　円の m 分体 K で分岐する素数は m の約数だけである．特に $m=p^n$ の場合は

$$\mathfrak{p}=(1-\zeta)=\{(1-\zeta)x \mid x\in\mathbb{O}_K\}$$

と置けば $\mathfrak{p}$ は K の素イデアルで

$$(p)=\mathfrak{p}^{\varphi(p^n)},\quad N_K\mathfrak{p}=p,$$

したがって (p) は $K/\mathbb{Q}$ で完全分岐である．

証明　$m=p$ (素数) の場合を扱う．$K=\mathbb{Q}(\zeta_p)$ の判別式は $D_K=(-1)^{(p-1)/2}p^{p-2}$ だったから，判別定理によって結果を得る．∥

§ 2. 2 次体の場合

円分体の相互法則から平方剰余の相互法則を導こう．そのためには 2 次体は円分体の部分体であることを示さねばならない．以下に ℓ を素数，$\ell^*=(-1)^{(\ell-1)/2}\ell$ として

$$\mathbb{Q}(\sqrt{\ell^*})\subsetneqq\mathbb{Q}(\zeta_\ell) \tag{2}$$

であることを証明する．なお，一般の素数を表すのに p を使いたいので，固定された素数を表すためには ℓ を使うことにする．

円分体と 2 次体の関係を論じるために次の**ガウス和**を導入する：

$$\tau_\ell=\sum_{j=1}^{\ell-1}\left(\frac{j}{\ell}\right)\zeta_\ell^j$$

ここに $\zeta_\ell=e^{2\pi i/\ell}$ とし，(j/ℓ) は平方剰余記号である．

定理 14.3　$\ell^*=(-1)^{(\ell-1)/2}\ell$ とすれば

$$\tau_\ell^2=\ell^*$$

が成り立つ．

証明　以下で x^* は $xx^* \equiv 1 \pmod{\ell}$ なる整数を表す．このとき $(x^*/\ell) = (x/\ell)$ である．

$$\begin{aligned}
\tau_\ell^2 &= \left(\sum_x \left(\frac{x}{\ell}\right)\zeta_\ell^x\right)\left(\sum_y \left(\frac{y}{\ell}\right)\zeta_\ell^y\right)\\
&= \left(\sum_x \left(\frac{x}{\ell}\right)\zeta_\ell^x\right)\left(\sum_y \left(\frac{-y}{\ell}\right)\zeta_\ell^{-y}\right)\\
&= \left(\frac{-1}{\ell}\right)\sum_{x,y}\left(\frac{xy}{\ell}\right)\zeta_\ell^{x-y}\\
&= (-1)^{\frac{\ell-1}{2}}\sum_{x,y}\left(\frac{x^*y}{\ell}\right)\zeta_\ell^{x(1-x^*y)}\\
&= (-1)^{\frac{\ell-1}{2}}\sum_z\left(\frac{z}{\ell}\right)\sum_x \zeta_\ell^{x(1-z)} \quad (\text{ここに } z = x^*y)
\end{aligned}$$

$$\sum_{x=1}^{\ell-1}\zeta_\ell^{x(1-z)} = \begin{cases} \ell - 1 & (z \equiv 1 \pmod{\ell}) \\ -1 & (z \not\equiv 1 \pmod{\ell}) \end{cases}$$

$$\begin{aligned}
\therefore\quad \tau_\ell^2 &= (-1)^{\frac{\ell-1}{2}}\left((\ell-1) - \sum_{z\neq 1}\left(\frac{z}{\ell}\right)\right)\\
&= (-1)^{\frac{\ell-1}{2}}\ell \quad \left(\because\ \sum_z \left(\frac{z}{\ell}\right) = 0\right)
\end{aligned}$$ ∥

上の命題から，

$$\tau_\ell = \pm\sqrt{\ell^*} \in \mathbb{Q}(\zeta_\ell)$$

という結果が従う．これによって，(2) が示された．なお符号 $\pm$ の決定はガウスを大いにてこずらせた問題で，結論は次の通りだが，本書では必要がないので証明は省略する：

定理 14.4 (ガウス)　$\ell^* = (-1)^{(l-2)/2}\ell$ とすれば

$$\tau_\ell = \sqrt{\ell^*}$$

以下，p は奇素数とする．まず円分体のフロベニウス写像と平方剰余記号との関係を述べる．アーベル拡大 $K/\mathbb{Q}$ において (p) は不分岐とし，(p) の素因子を代表的に $\mathfrak{p}$ とすると，そのフロベニウス写像 σ は

$$\alpha^{\sigma} \equiv \alpha^{p} \pmod{\mathfrak{p}} \quad (\forall \alpha \in \mathbb{O}_K)$$

を満たす．τ $(\in G(K/\mathbb{Q}))$ を作用させると

$$(\alpha^{\sigma})^{\tau} \equiv (\alpha^{\tau})^{p} \pmod{\mathfrak{p}^{\tau}}.$$

$G(K/\mathbb{Q})$ がアーベル群という仮定によって $\sigma\tau = \tau\sigma$ だから

$$(\alpha^{\tau})^{\sigma} \equiv (\alpha^{\tau})^{p} \pmod{\mathfrak{p}^{\tau}}.$$

ところで α が $\mathbb{O}_K$ をわたると α^{τ} も $\mathbb{O}_K$ をわたるから，上式は

$$\alpha^{\sigma} \equiv \alpha^{p} \pmod{\mathfrak{p}^{\tau}} \quad (\forall \alpha \in \mathbb{O}_K)$$

を意味している．すなわち σ は素因子 $\mathfrak{p}^{\tau}$ のフロベニウス写像でもある．(p) の素因子はすべて $\mathfrak{p}^{\tau}$ $(\tau \in G(K/\mathbb{Q}))$ の形をしているから，結局 (p) の素因子のフロベニウス写像はすべて一致し，(p) だけで定まることがわかった．そこで，これを

$$\left(\frac{K/\mathbb{Q}}{p}\right)$$

という記号で表すことにする：

$$\alpha^{\left(\frac{K/\mathbb{Q}}{p}\right)} \equiv \alpha^{p} \pmod{\mathfrak{p}} \quad (\forall \alpha \in \mathbb{O}_K)$$

補題　$(m, p) = 1$ ならば

$$\left(\frac{m}{p}\right) = 1 \iff \left(\frac{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}{p}\right) = e \quad (\text{恒等写像})$$

証明　フロベニウス写像が恒等写像なることは (p) が $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ で分解することだから，定理 11.10 と合せれば明らかである．‖

定理 14.5 (第 1 補充法則)

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

証明　オイラー規準を使って既に証明されているが，円分体論の中で別証を与える．$K = \mathbb{Q}(\sqrt{-1})$ とする．K は円の 4 分体である．

$$\left(\frac{-1}{p}\right) = 1 \iff \left(\frac{K/\mathbb{Q}}{p}\right) = e \quad (\text{補題より})$$
$$\iff p \equiv 1 \pmod{4} \quad (\text{分解定理より}) \quad ‖$$

定理 14.6 (平方剰余の相互法則)　p も q も奇素数とすると

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}}$$

証明　円の q 分体を $K, q^* = (-1)^{(q-1)/2}q$ と置くと $\sqrt{q^*} \in K$ であった. $\mathbb{Q}(\sqrt{q^*})$ に対応する $(\mathbb{Z}/q\mathbb{Z})^\times$ の部分群を H とする：

$$\begin{aligned} H &= \{x^2 \mid x \in (\mathbb{Z}/q\mathbb{Z})^\times\} \\ &= \{y \bmod q \mid \exists x; y \equiv x^2 \pmod q,\ (y,q)=1\} \end{aligned}$$

$$\begin{aligned} \left(\frac{q^*}{p}\right) = 1 &\Longleftrightarrow \left(\frac{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}}{p}\right) = e \\ &\Longleftrightarrow \left(\frac{K/\mathbb{Q}}{p}\right) \in G(K/\mathbb{Q}(\sqrt{q^*}\,)) \\ &\qquad \left(\because\ \ \left(\frac{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}}{p}\right) = \left(\frac{K/\mathbb{Q}}{p}\right)\Big|\mathbb{Q}(\sqrt{q^*}\,)\right) \\ &\Longleftrightarrow p \bmod q \in H \quad (\text{定理 14.1 系 2}) \\ &\Longleftrightarrow \exists x; p \equiv x^2 \pmod q \\ &\Longleftrightarrow \left(\frac{p}{q}\right) = 1 \end{aligned}$$

すなわち

$$\left(\frac{q^*}{p}\right)\left(\frac{p}{q}\right) = 1$$

が常に成り立つ.

$$\left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}\left(\frac{q}{p}\right) \quad \blacksquare$$

$(-1)^{(q-1)/2}$ という因子が現れるのは 2 次体が円の q 分体の部分体となる条件だったことがわかる. 法 p の話が法 q の話にひっくり返るのは p のフロベニウス写像を σ とすると $\zeta^\sigma = \zeta^p$ (ζ は 1 の q 乗根) なので $\sigma \in H$ は $p \bmod q$ が $(\mathbb{Z}/q\mathbb{Z})^\times$ の平方類, すなわち p が法 q の平方剰余ということと同値となることによるのである. つまり次のようである：

$$\left(\frac{q^*}{p}\right) = 1 \Longleftrightarrow\ p \text{ が } \mathbb{Q}(\sqrt{q^*}\,)/\mathbb{Q} \text{ で分解する } (f=1)$$

$$\Updownarrow$$

$$\left(\frac{p}{q}\right) = 1 \Longleftrightarrow\ p \text{ が } \bmod q \text{ では平方数}$$

$\Updownarrow$ の部分は $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ が巡回拡大であることとガロアの理論の基本定理によっている．

問題 (第 2 補充法則)

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

[ヒント]　$\sqrt{2}$ を含む最小の円分体を K とすると, K は円の 8 分体である：

$$K = \mathbb{Q}(\zeta),\quad \zeta = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i)$$

$$\therefore\quad K = \mathbb{Q}(\sqrt{2}, i)$$

$\mathbb{Q}(\sqrt{2})$ に対応する $(\mathbb{Z}/8\mathbb{Z})^\times$ の部分群は $\{\pm 1 \bmod 8\}$ である．

§ 3. 類体論とは？

類体論とは有理数体上で言えば円分体論, すなわち相互法則, 分解定理, クロネッカー–ヴェーバーの定理などである．K を代数体とすると K 上のアーベル拡大体は必ずしも 1 の冪根を K に添加した体とは限らぬところが $K = \mathbb{Q}$ の場合と根本的に違う点なのだが，それにもかかわらず円分体論の類似が成り立つところに面白さと不可思議さが秘められている．本節と次節で類体論についての結果を述べる．

K を代数体として，I_K によって $\{0\}$ 以外の分数イデアル全体のなす群, P_K によって $\{0\}$ 以外の単項イデアルのなす部分群を表し，$C_K = I_K/P_K$ とすると，イデアル類群 C_K は有限群となるのであった (定理 11.6).

ヒルベルトは，任意の代数体 K に対して，次の性質を有する拡大体 $\widetilde{K}$ が存在することを予想した (1898 年)：

$[\widetilde{K} : K] = n$ とするとき，K の素イデアル $\mathfrak{p}$ が単項イデアルであるためには $\widetilde{K}$ において完全分解すること，すなわち，

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$$

と n 個の素イデアルの積に分解されることが必要十分である.

さらにヒルベルトはこの $\widetilde{K}$(現在では, K の**絶対類体**と呼ばれる) に関して, 次の性質が成り立つであろうと (2,3 の実例を基に) 予想した：

(1) K の絶対類体は唯一である.

(2) $\widetilde{K}/K$ はアーベル拡大で $G(\widetilde{K}/K) \simeq C_K$, したがって $n = h_K$.

(3) $\widetilde{K}/K$ は不分岐拡大, すなわち分岐する素イデアルは存在しない.

(4) $\mathfrak{p}$ を K の素イデアルとするとき, $\mathfrak{p}^f$ が単項イデアルとなる最小の自然数 f を取ると, $\mathfrak{p}$ は $\widetilde{K}$ において

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \quad fg = n, \quad N_{\widetilde{K}/K} \mathfrak{P}_j = \mathfrak{p}^f$$

と素イデアル分解される.

[注意] $\mathfrak{a}^{h_K}$ は任意の $\mathfrak{a} \in I_K$ に対して単項だから (4) の f は存在する.

ヒルベルトがどうしてこのような予想を思い付いたのかはわからない. 高木先生は「偉大なるヤマカンだろう」と述べておられたように記憶している. 上の予想はフルトベングラーによって証明された (1907 年). 類体論の歴史は文献 [12], [14] に譲ることにして, ここではこれ以上触れないことにする.

円分体論とは (4) という類似があるのみだが, 実際には両者は高い立場から統合され, 次のように立体的・視覚的に表現されることになる.

定義 L/K をアーベル拡大とし, $\mathfrak{p}$ を L/K で不分岐な K の素イデアルとする. $\mathfrak{p}$ の L/K におけるフロベニウス写像を $\left(\dfrac{L/K}{\mathfrak{p}}\right)$ で表す. また $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$ に対しては

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \left(\frac{L/K}{\mathfrak{p}_1}\right)^{n_1} \cdots \left(\frac{L/K}{\mathfrak{p}_s}\right)^{n_s}$$

と定義する (ただし各 $\mathfrak{p}_j$ は L/K で不分岐な素イデアル).

[注意]　L/K がアーベル拡大であればフロベニウス写像が K の素イデアル $\mathfrak{p}$ の L における素因子の取り方に無関係に定まることは円分体の場合に見たのと同じく簡単にわかることである．しからば，$\mathfrak{a}$ の属する C_K の類を $\tilde{\mathfrak{a}}$ と表せば，先のヒルベルトの予想した (2) の同型写像：$C_K \longrightarrow G(\widetilde{K}/K)$ は

$$\tilde{\mathfrak{a}} \rightsquigarrow \left(\frac{\widetilde{K}/K}{\mathfrak{a}}\right)$$

によって実現される (絶対類体の場合におけるアルチンの一般相互法則)．特に $\left(\frac{\widetilde{K}/K}{\mathfrak{a}}\right) = e$ となる条件は $\mathfrak{a}$ が単項イデアル ($\tilde{\mathfrak{a}} = \tilde{1}$) であることである．また $\mathfrak{a}$ が素イデアル $\mathfrak{p}$ の場合を考えればフロベニウス写像の性質からヒルベルトの予想の (4) が必然的に導かれる．

これで，いくらか円分体の場合と似て来た．絶対類体の場合だけを取り上げても，類体論というのは不可思議な理論である．しかるに，その上，次の不可思議な定理が成り立つのだから，整数論が数学の女王と呼ばれるのも宜(むべ)なるかな：

定理 14.7 (単項化定理)　K のすべてのイデアルは絶対類体 $\widetilde{K}$ において単項イデアルとなる．すなわち，$\mathfrak{a}$ を K のイデアルとすれば

$$\exists A \in \widetilde{K}^{\times};\ \mathfrak{a} = (A) \quad \text{in } \widetilde{K}$$

ここに左辺の $\mathfrak{a}$ は正確には $\mathfrak{a}\mathbb{O}_{\widetilde{K}}$ のことであり，右辺の (A) は $A\mathbb{O}_{\widetilde{K}}$ のことであるのは言うまでもない．

有理数体 $\mathbb{Q}$ の場合は類数が 1 だから，その絶対類体 $\widetilde{\mathbb{Q}}$ は $\mathbb{Q}$ そのもので，単項化定理は自明に成り立っている．

単項化定理もヒルベルトの予想の中に含まれていたが，高木の類体論からは証明できなかった．アルチンが一般相互法則を使って問題を群論化してから，これもフルトベングラー (指揮者のフルトベングラーの従兄弟だそうである) によって 1930 年に解決された．類体論で高木に名を成さしめ，悔し

がったフルトベングラー (高木とはヒルベルトの相弟子) は単項化定理で一矢を報いたのだ，とは東洋の片田舎のスズメのハヤシたてるところである．

さて，K のイデアルは $\widetilde{K}$ で単項イデアルとなるけれども，$h_{\widetilde{K}} \neq 1$ ならば $\widetilde{K}$ には単項でないイデアルが存在する．このときはさらに $\widetilde{K}$ の絶対類体 $\widetilde{\widetilde{K}}$ を考えてみる．$h_{\widetilde{\widetilde{K}}} \neq 1$ ならば，さらに $\widetilde{\widetilde{K}}$ の絶対類体を考える．かく進行していけばいつかは (有限回で) 類数が 1 の代数体に達するであろうか？　これが**類体塔問題**と呼ばれる，この周辺に残されたほとんど唯一とも言える古典的大問題だったが，シャファレビッチとゴロッドによって否定的に解かれてしまった (1964 年)．すなわち無限に類体塔が続く代数体の例がみつかったのである：

たとえば，初期に与えられた例だが $K_0 = \mathbb{Q}(\sqrt{-2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17})$ とすると $K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_n \subsetneqq \cdots$ (ここに $K_{j+1} = \widetilde{K}_j$) が成り立つ．最近ではもっと簡単な例がいくつも見付かっているだろう．

§ 4.　類体論とは？(続)

さて円分体と絶対類体の双方を包含する理論である類体論の話を続けよう．K の $\mathbb{Q}$ 上の共役体を $K^{(1)}, \cdots, K^{(n)}(n = [K:\mathbb{Q}])$ とし，$K^{(1)}, \cdots, K^{(r)}$ は実数体 $\mathbb{R}$ の部分体，残りはそうでないとする．($K^{(1)} = K$ とは仮定しない．順序は適当に定めて固定する．)

定義　$\{j_1, \cdots, j_k\} \subseteqq \{1, \cdots, r\}$ とする．$\alpha, \beta (\in K^\times)$ に対して

$$\alpha \equiv \beta \pmod{\mathfrak{p}_\infty^{(j_1)} \cdots \mathfrak{p}_\infty^{(j_k)}} \iff \alpha^{(j_1)}\beta^{(j_1)} > 0, \cdots, \alpha^{(j_k)}\beta^{(j_k)} > 0$$

と定義する．(要するに共役体 $K^{(j_i)}$ $(i = 1, \cdots, k)$ に写すと $\alpha^{(j_i)}, \beta^{(j_i)}$ が同符号であることを表明する記号である．) $\mathfrak{p}_\infty^{(1)}, \cdots, \mathfrak{p}_\infty^{(r)}$ を K の**実無限素点**と言う．

次に $\mathfrak{m}$ を K の整イデアル $\mathfrak{m}_0$ と $\{\mathfrak{p}_\infty^{(1)}, \cdots, \mathfrak{p}_\infty^{(r)}\}$ の部分集合 (空でもよい) の積 $\mathfrak{m}_1$ との形式的な積とする：

$$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_1, \quad \mathfrak{m}_1 = \mathfrak{p}_\infty^{(j_1)} \cdots \mathfrak{p}_\infty^{(j_k)}$$

$I_K(\mathfrak{m})$ でもって $\mathfrak{m}_0$ と素な (つまり素イデアル分解したとき共通因子を有さない) K の分数イデアル全体のなす群を表す：

$$I_K(\mathfrak{m}) = \{\mathfrak{a}\,(\in I_K) \mid \mathfrak{a}, \mathfrak{m}_0 \text{は因子無縁}\}$$

また，$I_K(\mathfrak{m})$ の部分群 $S_K(\mathfrak{m})$ を

$$S_K(\mathfrak{m}) = \{(\alpha) \mid \alpha \equiv 1 \pmod{\mathfrak{m}}, \quad \alpha \in K^\times\}$$

によって定義する．ここに $\alpha \equiv 1 \pmod{\mathfrak{m}}$ は

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0}, \qquad \alpha \equiv 1 \pmod{\mathfrak{m}_1}$$

を意味することとする．

商群 $I_K(\mathfrak{m})/S_K(\mathfrak{m})$ を $C_K(\mathfrak{m})$ と記す．

[注意]　$\alpha, \beta \in \mathbb{O}_K$ とは限らないので正確には $\alpha \equiv \beta \pmod{\mathfrak{m}_0}$ の意味を定義する必要がある．$(\alpha - \beta) = \mathfrak{a} \cdot \mathfrak{b}$ ($\mathfrak{a}$ は $\mathfrak{m}_0$ の素因子の冪積，$\mathfrak{b}$ は $\mathfrak{m}_0$ と因子無縁) と表して $\mathfrak{m}_0 | \mathfrak{a}$ のとき $\alpha \equiv \beta \pmod{\mathfrak{m}_0}$ と記すことにするというのがその定義である．しかし mod $\mathfrak{m}_0$ の各類から整の代表を取れるので $\alpha, \beta \in \mathbb{O}_K$ と思っていても間違いはない．

命題 1　$\mathfrak{m} = \mathbb{O}_K (= (1))$ の場合は，

$$C_K(\mathfrak{m}) = C_K$$

証明　$I_K(\mathfrak{m}) = I_K$，また $x \equiv 1 \pmod{\mathfrak{m}}$ は $\mathfrak{m} = \mathbb{O}_K$ だから $x \in K^\times$ の意味．したがって $S_K(\mathfrak{m})$ は単項イデアル全体である．‖

$K = \mathbb{Q}$ の場合は共役体といっても $\mathbb{Q}$ だけだから $r = 1$ となる．$\mathfrak{p}_\infty^{(1)}$ のかわりに $\mathfrak{p}_\infty$ と記す．$a \equiv 1 \pmod{\mathfrak{p}_\infty}$ は $a > 0$ の意味にすぎない．

命題 2　$\mathbb{Q}$ において $\mathfrak{m} = (m)\mathfrak{p}_\infty$, m を自然数とすると，

$$C_\mathbb{Q}(\mathfrak{m}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$$

証明　$f : C_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times}$ を次のように定義する．

(a) を $C_{\mathbb{Q}}(\mathfrak{m}) = I_{\mathbb{Q}}(\mathfrak{m})/S_{\mathbb{Q}}(\mathfrak{m})$ の一つの類 A の代表とする．$(-a) = (a)$ だから $a > 0$ としてよい．このとき

$$f(A) = a \bmod m$$

と定義してみよう．($a \in \mathbb{Z}$ とは限らないが，$b \equiv c \pmod{m}$, $(c, m) = 1$ のとき $b/c \equiv 1 \pmod{m}$ と定義するなど適宜修正すればよい．)

まず $(b) \in A$, $b > 0$ とすると

$$\exists (c) \in S_{\mathbb{Q}}(\mathfrak{m});\ (ca) = (b)$$

$(c) \in S_{\mathbb{Q}}(\mathfrak{m})$ より $c > 0$ かつ $c \equiv 1 \pmod{m}$ としてよい．故に $ca = b$ ($\because$ $ca > 0$, $b > 0$) とあわせて $a \equiv b \pmod{m}$，これで f が well defined であることがわかった．f が群としての同型写像であることは簡単に示せるので読者に任せよう． ∥

上の二つの命題によって $\mathfrak{m}$ を法とするイデアル類群 $C_K(\mathfrak{m})$ が $(\mathbb{Z}/m\mathbb{Z})^{\times}$ と C_K とを包含する概念であることがわかった．$C_K(\mathfrak{m})$ が有限アーベル群をなすことは C_K がそうであることから容易に示せるが，証明は略する．

定義　$H_K(\mathfrak{m})$ を $C_K(\mathfrak{m})$ の部分群とする．L/K が $H_K(\mathfrak{m})$ の**類体** (class field) であるとは，次のことが成り立つときである：

L/K はガロア拡大であって，$\mathfrak{m}$ と素な K の素イデアル $\mathfrak{p}$ は $\mathfrak{p} \in H_K(\mathfrak{m})$ (正確に言えば，類 $\mathfrak{p}S_K(\mathfrak{m})$ が $H_K(\mathfrak{m})$ の元である) の場合，かつその場合に限って，L において

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n, \quad n = [L : K]$$

と完全分解する．

類体はドイツ語では Klassenkörper だが，高木先生の論文では Classencörper とある．古いドイツ語では C が K のかわりに使われたそうで，この

方が古典的で格好良いらしい．そう言えば Carl L. Siegel (ジーゲル) の本名は Karl L. Siegel なのだと彌永 (昌吉) 先生から伺ったことがある．誰かがパスポートをのぞいて見たのだそうな．

類体については次の諸定理が成り立つ：

定理 14.8　任意のアーベル拡大 L/K はある $\mathfrak{m}$ に関してある $H_K(\mathfrak{m})$ の類体である．

系 (クロネッカー–ヴェーバーの定理)　有理数体上のアーベル拡大はある円分体の部分体である．

この系は先の命題 2 から明らかである．

定理 14.9 (存在定理)　任意の $H_K(\mathfrak{m})$ に対して $H_K(\mathfrak{m})$ の類体がただ一つ存在する．

定理 14.10 (一般相互法則)　L を $H_K(\mathfrak{m})$ の類体とすると，

$$C_K(\mathfrak{m})/H_K(\mathfrak{m}) \simeq G(L/K),$$

しかもこの同型対応は $\mathfrak{a} \rightsquigarrow \left(\dfrac{L/K}{\mathfrak{a}}\right)$ から導かれる．ここに $\mathfrak{a} \in I_K(\mathfrak{m})$ とする．したがって

$$\mathfrak{a} \in H_K(\mathfrak{m}) \Longleftrightarrow \left(\frac{L/K}{\mathfrak{a}}\right) = e \quad (\text{恒等写像})$$

系 (分解定理)　素イデアル $\mathfrak{p} \in I_K(\mathfrak{m})$ は $\mathfrak{p}^f \in H_K(\mathfrak{m})$ なる最小の自然数 f に対して

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \quad fg = [L:K]$$

と L において素イデアル分解される．したがって $N_{L/K}\mathfrak{P}_j = \mathfrak{p}^f$ $(j = 1, \cdots, g)$ である．

問題　定理 14.10 から系を証明せよ．

定理 14.11　H_1, H_2 がともに $C_K(\mathfrak{m})$ の部分群であるとする．L_1, L_2 を H_1, H_2 の類体とするとき

$$L_1 \subseteqq L_2 \Longleftrightarrow H_1 \supseteqq H_2$$

問題　定理 14.11 をガロアの理論を用いて証明せよ．

定理 14.12　L/K が $H_K(\mathfrak{m})$ の類体であるとする．このような $\mathfrak{m}$ のうち因子の個数が最小になるように $\mathfrak{m}$ が取ってあるとすれば (こういう $\mathfrak{m}$ を L/K の**導手**という)，K の素イデアル $\mathfrak{p}$ が $\mathfrak{m}$ を割り切ることが L/K で $\mathfrak{p}$ の分岐する必要十分条件である．

ただし $\mathfrak{p}_\infty^{(j)}$ が $\mathfrak{m}$ の約因子のときは，$K^{(j)} \subseteqq \mathbb{R}$ だけれども $K^{(j)}$ 上の L に対応する拡大 $L^{(j)}$ は $L^{(j)} \subsetneqq \mathbb{R}$ であることを意味する．

例　$\mathbb{Q}(\sqrt{-1})$ の導手は (4) p_∞ で，$\mathbb{Q}(\sqrt{-1})$ は $H_\mathbb{Q}(4p_\infty) = S_\mathbb{Q}(4p_\infty)$ の類体である．これは $\mathbb{Q}(\sqrt{-1})$ が円の 4 分体だからである．$\mathbb{Q}(\sqrt{2})$ の導手は (8) である．この体は $S_\mathbb{Q}(8)$ の類体である．

以上で基本的な定理は述べ終わった．定理 14.10 の，同型対応が $\mathfrak{a} \rightsquigarrow \left(\dfrac{L/K}{\mathfrak{a}}\right)$ で実現される，という部分がアルチンによって 1927 年に証明された一般相互法則と呼ばれる，高木の類体論 (1920 年) の画竜点睛と称えられた大定理である．高木の類体論でも同型定理，分解定理等の主要な結果が得られていたのだが，相互法則によって，これらが簡単な系として示せることになった．

問題　$\mathfrak{m} = (1)$ のとき定理 14.9，定理 14.10，系，定理 14.12 がちょうど絶対類体の諸定理を尽していることを確認せよ．

問題　$K=\mathbb{Q}$ の場合，定理 14.10，系，定理 14.11，定理 14.12 がちょうど円分体論を表していること，および定理 14.8 がクロネッカー–ヴェーバーの定理を表していることを確認せよ．

算術級数の定理の一般化として，次の定理が成り立つ：

定理 14.13　$C_K(\mathfrak{m})/H_K(\mathfrak{m})$ の各類は無数の素イデアルを含む．

類体論が円分体論のはるかな一般化であるとは言うものの，以上述べた類体論の諸定理が円分体論に比して一点だけ劣る点がある．それは円分体は $\mathbb{Q}(\zeta_m)$，ここに ζ_m は 1 の原始 m 乗根，たとえば $\zeta_m=e^{2\pi i/m}$，すなわち e^z の m 等分値，という様にきわめて具体的に，目に見える形で与えられるのに対して，$S_K(\mathfrak{m})$ に対応する類体と言えども，K にどんな数値を添加して得られるのか，一向に具体性がないという点である．類体論は，この段階では，いわゆる理論であって具体性にとぼしい．これについては，次の有名な問題があった：

クロネッカーの青春の夢 虚 2 次体

$$K=\mathbb{Q}(\sqrt{-m}\ )\quad (m>0)$$

の場合，K 上の任意のアーベル拡大は K に 1 の冪根とモジュラー関数 (ある種の楕円関数) の特殊値を添加した体に含まれるのではないか?

4 次までの方程式は冪根 (すなわち $\exp\dfrac{\log a}{n}$) で解けたが，5 次方程式は楕円関数の値を必要とした，という物語を思い起させるではないか．まさしく「青春の夢」(Jugentraum) と呼ぶにふさわしい予想だが，この青春の夢はいくらかの (さらにある種の楕円関数の m 分点を添加する必要があるという) 修正を施すことによって解決された．これを解決したのも高木貞治である (1920 年)．しかるに，ハッセが青春の夢を解決したと述べている欧文の書

物を見かけることがあるのは困った認識不足である．ハッセは虚数乗法論を整理して高木の解決を紹介したに過ぎない．

Jugentraum に関する概説や歴史についても河田 [11]，足立・三宅 [12] を紹介するにとどめよう．なお，Jugentraum は，「一般的に与えられた代数体 K のアーベル拡大は何かある特殊関数 $f(z)$ の特殊値 $f(z_0)$ を添加して得られる」というさらに誇大妄想的な夢に昇華することは誰でも思い付くことだろうが，これは有名な「ヒルベルトの第 12 問題」として知られ，虚 2 次体の場合以外はかなり部分的な結果が知られているのみである．アーベル体論が類体論の完成によって終わったと思うのは一知半解である．

類体論とかけて何と解く．ゲーリー・クーパーと解く．その心は？ 壮大な外観の割りには中はがらんどう．ゲーリー・クーパーについて，多くの人が「中に設備がほとんど収まってない大聖堂を思わせる」と語っていることからの連想である．ちなみに私はゲーリー・クーパーが大好きであることを断っておく．

代数関数論からの類推があったにしてもヒルベルトの (妄想的とも教祖的とも言える) 洞察力があり，一方ヴェーバーによる一般的な類体の定義がすでにあったにしても，そうした予想をはるかに凌駕する理論を創り上げた高木と一般相互法則によって高木の類体論を構造化したアルチンの業績は永遠に語り継がれていくに違いない．そう言えば，来年 (2010 年) は高木先生が亡くなられて 50 年，類体論が発表されて 90 年という記念すべき年なのだそうである．今年 (2009 年) は本書の初版が出て 30 年，… というのは悪のりだが，何かの因縁である，ということにして筆を擱(お)く．

付録　集合論のイロハ

§1. 集合論の公理系 ZFC

等号記号 $=$ を備えた数学言語において集合論の公理系を考える (等号公理については第 3 章 §2 参照). 基本となる数学の関係記号は所属を表す $\in$ だけである. 以下では

$$a, b, \cdots, x, y, \cdots, A, B, \cdots,\ X, Y, \cdots$$

などの文字は集合を表す変数とする.

なじみ易さを考えて, 小文字と大文字を分けて使っているが, 現代数学では, 数も図形も関数もすべて集合として定義されるので, はっきり言えば, **集合** (set) と**元** (element) **とは同義語**であって, 見方によって元として扱ったり, 集合として扱ったりするに過ぎないことを, あらかじめ理解しておいてほしい. つまり, 文字はすべて小文字にしたって構わない, むしろその方が一貫性があるとも言えるのである.

φ を論理式として, $\{x \mid \varphi(x)\}$ という形式を**クラス**という. クラス $\{x \mid \varphi(x)\}$ が集合をなすとは,

$$x \in X \iff \varphi(x) \text{ が成り立つ}$$

を満たす集合 X が存在することをいう. 正確を期して言うなら, クラスという概念は, 本節で述べる集合論 ZF では, なくて済ませられる補助的概念である. クラスを真の対象とする集合論については §3 参照. クラスは必ずしも集合をなさない. たとえば,

$$V = \{x \mid x = x\}$$

はすべての集合のなすクラスで, この V は真のクラスである (すなわち集合

ではない)．この V を宇宙 (ユニバース) と呼ぼう．

こうしたものを扱ってはいけないかのごとく誤解している人がいるかもしれないが，真のクラスを「集合として扱う」と明白に矛盾を生じるのであって，矛盾を起こさない限り，どんな概念であろうと数学の (広く言えば，理性の) 対象として扱ってはならない訳がないことを知るべきである．そればかりか，以下の公理系の述べ方を見るとわかるように，どのようなクラスが集合と呼べるかを規定するのが，集合論の公理系であると言うことさえできる．

1. (**外延性公理**) $\forall x(x \in X \Leftrightarrow x \in Y) \Longrightarrow X = Y$

論理式 $\forall x(x \in X \Rightarrow x \in Y)$ を $X \subseteqq Y$ と記せば，外延性公理は

$$(X \subseteqq Y) \wedge (Y \subseteqq X) \Longrightarrow X = Y$$

と書ける．

2. (**分離公理**) φ を論理式とすると，任意の集合 X に対して

$$\{x\ (\in X) \mid \varphi(x)\} = \{x \mid (x \in X) \wedge \varphi(x)\}$$

は集合である．

対象を集合の元に限定するなら，クラスが集合として確定することを保証するのが分離公理である．クラス $\{x \mid x \notin x\}$ などが集合をなすと考えると矛盾を起こすことから思い付かれた公理である．

3. (**空集合公理**) $\{x \mid x \neq x\}$ は集合である．

何か一つ集合がなければ始まらないので，この公理を置く．外延性公理によって，この集合はただ一つ存在することがわかるので，これを空集合と呼び，

$$\varnothing$$

と記す．主として数を考えているときは，これを 0 と表す．

クラスの記号を使わないなら，空集合公理は「$\forall x\ (x \notin a)$ を満たす a が存在する」と表現される．以下の諸公理についても同様である．

4. (**対集合公理**)　任意の a, b に対して，

$$\{x \mid (x = a) \vee (x = b)\}$$

は集合である．

この (a, b に対して一意的に定まる) 集合を

$$\{a,\ b\}$$

と表す．$a = b$ のときには，

$$\{a\}$$

と記す．

5. (**冪集合公理**)　任意の X に対して

$$\{x \mid x \subseteqq X\}$$

は集合である．

この (X に対して一意的に定まる) 集合を X の冪集合と言って $P(X)$ と記す．

6. (**和集合公理**)　集合 X に対して

$$\{x \mid \exists y\,(x \in y \wedge y \in X)\}$$

は集合である．

外延性公理によってユニークに定まるこの集合を X の和集合と言って

$$\bigcup X$$

と記す．普通の数学では X が集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ という形をしていて，$\bigcup_{\lambda\in\Lambda} A_\lambda$ と書かれる場合が多い．しかし，この集合族の書き方は集合 Λ で定義された関数 (写像) の概念を使っていることには注意しておく必要がある．

集合 X, Y に対して $\bigcup\{X, Y\}$ を $X\cup Y$ と記し，X と Y の和集合という．

集合 X $(\neq\varnothing)$ に対して $\{x \mid \forall y\in X\,(x\in y)\}$ は集合をなす．$a\in X$ を一つ取れば，これは $\{x\,(\in a) \mid \forall y\in X\,(x\in y)\}$ とも書け，分離公理によって集合となるのである．この集合を X の共通部分集合といって

$$\bigcap X$$

と表す．$X=\varnothing$ のときは，条件 $\forall y\,(y\in X\Rightarrow x\in y)$ は自明に満たされるので $\bigcap\varnothing=V$ である．

対集合公理以下の公理は，集合が与えられたときに，新たに集合を生み出す仕組みを述べている．存在を保証された唯一の集合である空集合 $\varnothing$ から，次のようにして次々集合が生み出される．

$$P(\varnothing)=\{x\mid x\subseteqq\varnothing\}=\{\varnothing\}$$

この $\{\varnothing\}$ を 1 と記す．また

$$P(1)=P(\{\varnothing\})=\{x\mid x\subseteqq\{\varnothing\}\}=\{\varnothing,\{\varnothing\}\}=\{0,\ 1\}$$

である．これを 2 と記す (以下続く)．また和集合公理を使えば，

$$\bigcup\{\{a,\ b\},\ \{c\}\}=\{a,\ b\}\cup\{c\}$$

として $\{a,\ b,\ c\}$ が定義される．

7. (**置換公理**)　クラス F を関数 (写像) とし，X を集合とすると，その値域 $\{F(x)\mid x\in X\}$ は集合である．

ここに関数 F と言っている内容を説明する．論理式 $\varphi(x,y)$ に対して

$$\forall x \in X \exists ! y(\varphi(x, y))$$

が成り立っているときに，$x \in X$ に対して

$$y = F(x) \Longleftrightarrow \varphi(x, y)$$

と定義する．ここに ∃! は「ただ一つだけ存在する」という意味である．

分離公理は置換公理から証明できるが，分離公理という名称をしばしば使うので，一応別に掲げておく．集合論を最初に公理化したツェルメロの公理系には置換公理はなかった．置換公理の追加はフレンケルの貢献による．

以上の公理を使えば，順序対 (a, b) の定義が可能となる：

$$(a, b) = \{\{a\},\ \{a, b\}\}$$

このとき

$$(a, b) = (c, d) \Rightarrow a = b \wedge c = d$$

は容易に証明できるから，読者に任せる．これを使って直積 $X \times Y = \{(x,\ y) \mid (x \in X) \wedge (y \in Y)\}$ が定義される．$X,\ Y$ が集合の場合に $X \times Y$ が集合となることを示す必要があるが，$x \in X,\ y \in Y$ のとき $\{x\} \subsetneqq X \cup Y,\ \{x, y\} \subsetneqq X \cup Y \quad \therefore \quad \{x\}, \{x, y\} \in P(X \cup Y) \quad \therefore \quad \{\{x\}, \{x, y\}\} \subsetneqq P(X \cup Y)$．故に $(x, y) \in P(P(X \cup Y))$ だから，分離公理が使えて問題はない．

a に対して a' を

$$a' = a \cup \{a\}$$

によって定義する．a を数として扱う場合は a' を往々にして $a + 1$ と記す．

8. (**無限公理**)　論理式 $(0 \in X) \wedge \forall x(x \in X \Rightarrow x' \in X)$ を $C(X)$ と置くと，$C(X)$ を満たす X が存在する．

無限公理は無限に多くのもの (集合) が存在することを主張しているのではない．

$$0,\ 1 = \{0\},\ 2 = \{0,\ 1\},\ 3 = \{0,\ 1,\ 2\},\ \cdots$$

と定義すれば，無数に多くのものが存在することは明らかである (アリストテレスの言うところの潜在無限である).

> Notice that the Axiom of Infinity does not say that there are infinitely many things. Indeed, without it, we have infinitely many things $0, 1, 2, 3, \cdots$. It is just with the existence of a single set which is infinite that the typical and sometimes bizarre character of set theory begins. (Vaught[15])

$\mathbb{N} = \bigcap\{X \mid C(X)\}$ と置く．無限公理と分離公理によって，$\mathbb{N}$ は集合である．$\mathbb{N}$ は $C(X)$ を満たすような最小の集合であるということができる．$\mathbb{N}$ の元を**自然数**という．順序集合としての $\mathbb{N}$ はしばしば ω と表される．

$C(X)$ ばかりでなく，さらに任意の $x\ (\neq \varnothing) \in X$ が先行する元を持つ，つまり $x = y'\ (y \in X)$ と表せる，すなわち

$$\forall x \in X[x \neq \varnothing \Rightarrow \exists y \in x\,(x = y')]$$

を満たす X の存在を無限公理として採用すれば，この X を $\mathbb{N}$ とすることもできる．しかしその一意性の証明などに正則性公理が必要となる．

9. (**正則性公理**)　任意の $X\ (\neq \varnothing)$ に対して

$$x \cap X = \varnothing$$

を満たす $x \in X$ が存在する．

以上の公理系を集合論 ZF と言う．

正則性公理はちょっと意味が捉えにくい．普通の数学では使われないが，順序数のところで後述するように，集合論を整然と展開するのに必要だとされている．しかしながら，$a \in a$ とか，$\{a, b\} = a$ といった現象を排除するのが正則性公理の役目であると言えば受け入れ易いのではないだろうか．

(実際，$a \neq \varnothing$ のとき $x \cap \{a\} = \varnothing$ なる $x \in \{a\}$ が取れる．このとき $x = a$ であるから $a \cap \{a\} = \varnothing$．故に $a \notin a$ が従う．) 上記のような「異常」現象はわれわれ数学者の「感覚」や「常識」に反するが，そんな感覚は当てにならない後天的な知識を背景にして作り出されたものだとはいえ，要するにわれわれは正則性公理を当然のこととして暗黙のうちに認めているのである．

さて X $(\neq \varnothing)$ を $\varnothing \notin X$ なる集合とする．X を定義域とする関数 F が

$$\forall x(\in X)[F(x) \in x]$$

を満たすとき，F は X の**選択関数** (choice function) と呼ばれる．

10. (**選択公理**)　$\varnothing \notin X$ なる任意の集合 X $(\neq \varnothing)$ に対して選択関数が存在する．

ZF に選択公理を加えて集合論 ZFC と言う．

§2. 選択公理と同値な命題

順序数という概念は普通の数学 (数学基礎論以外の数学という意味) を学んでいる人間にはなじみが薄いため，選択公理と整列原理の同値性などの証明は順序数を使わないのが一般的である (たとえば,彌永, 小平 [2], 足立 [21]). しかし，順序数のごく基礎を知っていると，同値性の証明はあっけないほど簡単であるばかりか，なぜ同値なのかが腑に落ちる．この「証明が腑に落ちる」というのは数学の理解にとって極めて重要であることはだれにも異存がないところだから，ここでほんの定義だけだが順序数を導入し，同値性の証明に利用することにしよう．

まず，任意の部分集合 $\neq \varnothing$ が最小元を持つような順序集合を整列集合と称するという定義を思い出していただきたい．加法・乗法の演算を備えた集合としての $\mathbb{N}$ を拡大した概念が $\mathbb{Z}$, $\mathbb{Q}, \cdots$ であり，整列集合としての ω の性質を拡大したものが (超限) 順序数という概念である．

定義　集合 α が (フォン・ノイマン式の) **順序数**であるとは，次が満たされることである：

1. (整列性)　α は関係 $\in$ で整列集合をなす．
2. (推移性)　$x \in \alpha \wedge y \in x \Longrightarrow y \in \alpha$

$0, 1, 2, \cdots$ は順序数である．その後

$$0, 1, \cdots, \omega, \omega+1, \cdots, \omega\cdot 2, \omega\cdot 2+1, \cdots, \omega\times\omega, \cdots, \omega^{\omega}, \cdots$$

と続く．順序数の和や積の定義はここでは省略する．辞書式順序という言葉を知っていれば自分で考えることも大して難しいことではない．順序数の全体のなすクラス On は集合ではない (ブラリ・フォルチのパラドクス)．しかし $\in$ は On の全順序であり，任意の空でないサブクラスは最小限を持つという意味で整列されている．今後 $\alpha, \beta \in On$ に対して $\alpha \in \beta$ を $\alpha < \beta$ と記す．

まず，超限帰納法によって関数 (写像) が定義できることを証明しよう：

定理 A.1 (超限回帰定理：超限帰納法による関数の定義)　G を関数 (クラス) とすると，

$$F(\alpha) = G(F|\alpha)$$

を満足する On 上で定義された関数 (クラス) F が一意的に存在する．ここに $F|\alpha$ は F の α への制限である．

証明　K をクラス

$$\{f \mid \exists\alpha[(f \text{ は}\alpha\text{上の関数}) \wedge (\forall\xi < \alpha)[f(\xi) = G(f|(\xi))]]\}$$

によって定義して，$F = \bigcup K$ と置く．このとき F が On 上の関数であることは容易に示される (詳細は [16], p.42 参照)．∥

第 6 章で述べたように，次の定理が成り立つ：

定理 A.2　次の 3 命題は同値である (すなわち集合論 ZF からお互いを証明できる)：

1. (**選択公理**)　空でない集合 X ($\not\ni \varnothing$) の選択関数が存在する．
2. (**整列原理**)　任意の集合に整列順序を入れることができる．
3. (**極大原理**)　帰納的順序集合は極大元を持つ．

証明の考え方　順序数 $0, 1, 2, \cdots, \omega, \cdots$ を順々に X の元に対応させていくと，いつかは X のすべての元に順序数が割り振られる．そうでないと，集合 X が On と対等なサブクラスを持つことになるからである．これで 1. ⇒ 2. が証明される．1. ⇒ 3. も考え方は全く同じである．

証明 (定理 A.2 の証明)

2. ⇒ 1. は自明．集合 $\bigcup X$ を整列し，各 $x\,(\in X)$ の最小元を取れば，それが選択関数となっているからである．

1. ⇒ 2. X ($\neq \varnothing$) を整列させたい集合とする．f を $P(X) - \{\varnothing\}$ の選択関数とする．理解を易しくするというだけの理由によって $a \notin X$ を一つ選んでおく．

超越帰納法による関数の定義によって，On をわたる数列

$$a_\alpha = \begin{cases} f(X - \{a_\xi \mid \xi < \alpha\}), & \{a_\xi \mid \xi < \alpha\} \subsetneqq X, \\ a, & \{a_\xi \mid \xi < \alpha\} = X \end{cases}$$

を定義する．$\{a_\xi \mid \xi < \alpha\} = X$ となる $\alpha \in On$ は必ず存在する．そこで

$$\theta = \min_\alpha \{X = \{a_\xi \mid \xi < \alpha\}\}$$

と置けば，θ は順序集合なのだから，

$$a_\alpha \prec a_\beta \Longleftrightarrow \alpha < \beta \tag{3}$$

という順序関係の導入によって X が整列集合になることは明らかである．

1. ⇒ 3. $(X, \prec)$ を空でない帰納的順序集合とし，f を $P(X) - \{\varnothing\}$ の選択関数とする．

$$W_\alpha = X - \{x\,(\in X) \mid \forall \xi < \alpha\ (a_\xi \prec x)\}$$

と置く．超限帰納法による関数の定義によって

$$a_\alpha = \begin{cases} f(W_\alpha), & W_\alpha \neq \varnothing, \\ a, & W_\alpha = \varnothing \end{cases}$$

と定義する (a は $a \notin X$ なる固定した元)．そして

$$\theta = \min_\alpha \{W_\alpha = \varnothing\}$$

と置けば, (3) と同じ関係が成り立つ．全順序集合 $\{a_\xi \mid \xi < \theta\}$ ($\subseteqq X$) は，X が帰納的であることによって，上界 $m \in X$ を持つ．仮に $a_\xi < m$ $(\forall \xi < \theta)$ が成り立つなら，$m \in W_\theta$ となって $W_\theta = \varnothing$ に矛盾するので $\exists \alpha < \theta$ $(a_\alpha = m)$ を得る．これは m が唯一の上界，したがって極大元であることを示している．

3. $\Rightarrow$ 1. は典型的なツォルンのレンマの適用例なので省略．‖

最後に，正則性公理に触れておく．超限帰納法を使って,

$$\begin{aligned} V_0 &= \varnothing \\ V_\alpha &= \bigcup_{\beta<\alpha} V_\beta \quad (\alpha\text{が極限順序数のとき}) \\ V_{\alpha+1} &= P(V_\alpha) \end{aligned}$$

と定義する ($\alpha \neq 0$ であって $\alpha = \beta + 1$ となる β が存在しないときに α は極限順序数であると言う).

$V_0 = \varnothing$ の後は,

$$V_1 = \{0\},\ V_2 = \{0,1\}, V_3 = \{0,1,2,\{1\}\}, \cdots, V_\omega = \bigcup_{n\in\omega} V_n, \cdots$$

という風に続いていくのだが,「こうして作られる集合だけが集合である」という主張は正則性公理と同値である：

定理 A.3　正則性公理 $\Longleftrightarrow V = \bigcup_{\alpha \in On} V_\alpha$

証明は，とりわけ難しくはないが，専門書に譲り，ここでは述べない．

$\varnothing$ から作られる「筋目の正しい」集合だけを対象とするというのは集合論を美しく簡潔に展開するためには必要だが，こんなことで良いのかという気もする．一方では，以前述べたように，たとえば，

$$\{a,\ b\} = a$$

というようなことが生じるのは「われわれの理性に反する」と考える人が多いだろう．正則性公理はこうした「異常現象」が起きないことを保証してくれる．したがって，素朴な立場の，言い換えれば，集合について深刻に考えたことがないわれわれ一般の数学者は正則性公理を暗黙裡に認めているとも言えるのである．

§3. 集合論 BGC

本節では，クラスを公理系に取り込んだ集合論を記述する．ZF が先述してあるので簡単に述べる．B はベルナイス (Bernays), G はゲーデル (Gödel) の頭文字である．

変数は集合とクラスの二つのタイプがあり，小文字は集合を，大文字はクラスを表す．

A. 1. 集合はクラスである．

2. $X \in Y$ ならば X は集合である．
3. (外延性公理)：$\forall u\,(u \in X \Leftrightarrow u \in Y) \Rightarrow X = Y$.
4. (空集合公理)：空集合 $\varnothing$ が存在する．
5. (対集合公理)：任意の x, y に対して対集合 $\{x, y\}$ が存在する．

B. (分離公理)：φ を論理式とし，$\exists, \forall$ は $\exists x$, $\forall y$ のように小文字しか束縛しないものとするとき，任意の $X_1, \cdots, X_n$ に対して

$$Y = \{x \mid \varphi(x, X_1, \cdots, X_n)\}$$

を満たす Y が存在する．すなわち任意の $X_1, \cdots, X_n$ に対して

$$x \in Y \Longleftrightarrow \varphi(x, X_1, \cdots, X_n)$$

C. 1. (無限公理)：無限集合が存在する．

2. (和集合公理)：任意の x に対して和集合 $\bigcup x$ が存在する．

3. (冪集合公理)：任意の x に対して冪集合 $P(x)$ が存在する．

4. (置換公理)：クラス F が関数であれば，$\{F(z) \mid z \in x\}$ は集合である．

D. (正則性公理)：任意の X に対して，$X \neq \varnothing$ ならば

$$x \cap X = \varnothing$$

を満たす $x \in X$ が存在する．

E. (選択公理)：$F(x) \in x$ が任意の $x\,(\neq \varnothing)$ に対して成り立つ関数 (クラス) F が存在する．

以上が集合論 BGC である．公理 E は $V - \{\varnothing\}$ の選択関数が存在するという強い形になっていることに注意しよう．公理 E (クラス版の選択公理) は次と同値である．

極大原理 (クラス版)　順序 $<$ を持つクラス X が「任意の全順序部分集合は上界を持つ」という帰納的性質を満たすならば，X は極大元を持つか，あるいは全順序をなす真の部分クラス Y を持つ．

証明は, 定理 A.2 において選択公理から極大原理を導いた証明に, 定理 A.3 (すなわち，どんな集合もある V_α の元であるということ) を組み合せれば簡単に得られるが，イロハの段階を超えつつあるので，これは読者の研究に任せることにしよう．

特別付録　赤々と沈みゆく太陽を見る

本書には，倉田令二朗さんや森毅さんといった個人名が登場するが，なじみの薄い読者も多かろうことを考え，いくらかでも雰囲気を知っていただくために，倉田さんに対する追悼文 (『万人の学問をめざして——倉田令二朗の人と思想』(日本評論社) 収録) を加筆・修正の上，転載させていただくことにした．

倉田令二朗さんに初めてお会いしたのは私が早稲田に来た年 (1972 年) の次の年か，その次の年で，木下素夫さんの紹介による．同時に，杉浦光夫さん，斎藤正彦さん，森毅さん，福富節男さん，清水達雄さんたちとも知り合いになった．私の人格形成において最も大きな影響を及ぼした時期であり，人たちである．

倉田さんに二人だけで会ったのは，恐らく 2 年連続で九大の集中講義に呼ばれて類体論の講義をしたときに待ち合わせたとか，厚木にいたころに家に泊まっていただいたというような，ほんの数回の機会であって，その他は先述の人たちや小島 順さん，廣瀬健さんといった同僚たちと一緒に酒席で同席したというのがほとんどである．しかも私はこの人たちより 10 歳以上若く，後から仲間に加えてもらった関係で，倉田さんの物まね小僧としての桁外れの才能や人を魅了してやまない座談の冴え，幅広い勉強熱心振りなど，何かを書こうと思っても，大抵は『破天荒の人 倉田令二朗』に収録された追悼文の中に含まれていて，私だけが知っている逸話や倉田さんに対する見方というようなものはほとんどない．

彼ら仲間 (引用のために Z 会とでも名付けよう：彼らが学生の時代には SSS と呼ばれる組織があったそうだが，SSS がそのまま続いて Z 会という親睦会になったと考えればわかり易い．雰囲気はそのまま維持されていた) が

集団として持っている歴史的意義といったものを私はしばしば感じるところなのだが，そのことに直接的に触れられた文章は読んだ記憶がないので，そういうことを記すことにしよう．

倉田さんが亡くなられたとき感じたのは，ある時代精神がはっきりと終わりを告げていくということだった．終戦直後から10年ばかりの間，日本には自由と希望と活気がみなぎっていた (野坂昭如や開高健の小説に活写されているような) 時期があった．私どもが小学校や中学校のころ，自由の履き違えという言葉を先生からよく聞かされたものである．中には，オーバーコートを着たままで授業する教師がいたりもした．学校の先生も軍隊帰りが多かった．「あの人には戦場で肩に背負われて逃げたから頭が上がらない」とか，「俺はロケットを付けた飛行機でポーンと飛び出して体当たりする練習ばかりしてたんだ」とか，「ああいうなで肩の野郎は (軍服の) 肩章が似合わんね」とか，「チャンコロは数が多い．数万人が川に飛び込んで死に，それを橋にして皆で川を渡る」とか，「ロスケは馬鹿だから云々 (聞くに堪えない言葉が続く)」といった雑談ばかり記憶にあって，まともな授業の方は記憶に薄い (そんなものだとは思うが)．共産党が自由と民主と進歩を象徴する政党として，弾圧に会いながらも知識人から支持されていた．実際には，共産党が自由を象徴するはずもなく，自由な社会が実現されるというのも幻想に過ぎなかった．世の中は均一化した，出る杭は打たれる，長いものには巻かれろ式の世間知が幅を利かせる，また再挑戦の許されない，管理社会へと最初は徐々に，しかし時が経つにつれ急速に，滔々と変貌していった．

その中にあって，Z会はいつまでも自由の雰囲気を漂わせていた．世の中の流れとの違いが浮き彫りになるにつれ，浮世離れした集団になっていったとも言えよう．木下さんは授業中，「すまん，一本だけ吸わせてくれ」とたばこを吸ったりされたものだが，そうした終戦直後の雰囲気のなごりをいつまでも絶やさず持ち続けたのがZ会であった．「私は君を教えたことがないのだから先生と呼ぶのはやめてくれ．先生，先生と呼ぶ根性が私は嫌いなんだ」と木下さんに注意されて以来，私は彼らを先生付けで呼ぶことは止めた．ま

た，彼ら自身先生と呼び合ったりすることもなかった．少々年が違っても木下とか倉田とか，ちょっと遠慮のある場合は，木下さんなら，たとえばホツさんとあだ名で呼んでいた．しかし倉田さんのような天衣無縫の自由人を，不作法な礼儀知らずとみなし，敬遠し，蔭で蔑んでいる秩序と序列が好きな人も世間にはいないではない (つまり，数多い).

皆で集まると，議論が盛んになった．ここで披露するために読書をしているのではないかとも思えるほど，皆さん本読みであった．木下さんや倉田さんの追悼集を読むとそういう雰囲気が十分に理解できるだろう．私も廣瀬健さんの追悼集で「早稲田の数学科が一番輝いていた頃」という文章を書き，Z会の影響が早稲田の数学科にまで及んでいた様子を記した．

一人ひとりを見ると，際立つというほどでもなく，ちょっとうるさい変わり者の，スノッブと言えば一番的確に評価できるような人がZ会の飲み会にいると生き生き，潑剌と輝いて見えるのが，まったく不思議であった．

あえて名付ければ，「戦後リベラリスト」というのが彼らには一番ふさわしいように思う．今となってはわかるのだが，左翼というのとはまったく違う．どういう意味ででも原理主義者では絶対にない．世の中には相手にレッテルを貼って分類すれば，ほとんど自分の頭で考える必要がなくなるたぐいの，十把一からげにしては正しくないが，一種の宗教団体であって，会員は思考停止を特徴とする組織が多い．

Z会といえども一つの集団であるからには，自由と民主主義に対する思い入れが一種の固定観念になっているような人がいないわけではないが，会員の多くはあくまで自分という芯を持っていながらも，底知れぬほど理解力があり，包容力があり，人を見る目があり，人間が柔軟であった．要するに，狂信的とか，党派的とか，常識的というのと対極に位置した人たちであった．それに何より，知的好奇心が全身から発散していた．

木下さんは仲間から「われらがヒルベルト」と呼ばれるほどの数学的力量を備えながらも，万事にわたって知識が深いため人から恐れられたものだったが，人前に姿を現すこと，名前が人に知られることを極端に嫌う人であった．

杉浦さんは，江戸期の儒者に関する論文を書くほど博覧強記でありながら，私のように無知な人間にも対等に付き合って意見を求める，驚嘆すべき公平さを身に備えていた．(杉浦さんに嫌われるような人間というのはどんな人格の人なのだろう？)

倉田さんは，わが親友茅嶋洋一の伝習館闘争 (表向きは，教科書を使わないで授業をしたという理由で三人の教師が高校を懲戒免職になったことを発端とする国を相手の裁判で 30 年間続いた) の後援会長を務めるなど，終生反権力人としての姿勢を貫いた．(しかし結局茅嶋は，最後まで節を曲げなかった茅嶋だけが，敗訴となって裁判は終った．)

岡田裕之さん (経済学者) による木下さんへの追悼文は「だが友の死は――木下よ，僕ははじめて知る，自らの滅びであることを．僕はいま赤々と沈みゆく太陽を見る」という感動的な言葉で締め括られる．わたしはこれは木下さん個人に対する弔辞としてではなく，木下さんが象徴する時代精神，具体的に言えば，Z 会やその周辺に象徴される精神に対して述べられた言葉であると考えたい．彼らを尊敬し，生き方，考え方の規範としてきた私にとって，今や太陽はほとんど沈みきった，と言える．

さらに言葉を変えて言おう．与えられたものであろうと，なかろうと，曲がりなりにも真の自由があった時代がほとんど終わりを告げたのを強く感じるのである．

参考文献

本書を書くに際して，参考にしたか，あるいは言及した文献のみを掲げる．そのうちには絶版，ないしは品切れになっているものもあるが，いつか復刊されることを希望する．この 20 年ばかりの間に刊行された本については，本書の内容・程度から言って言及しなかったものが多い．あしからず．

代数系に関しては以下の通り：

[1] ファン・デル・ヴェルデン，現代代数学，東京図書 (原著；1937, 1940: 銀林浩訳 1959, 1960)

いくら古くなったと言っても，歴史的名著としての地位は揺るがない．(ドイツにいた専門家ならともかく) 世間的に言えば，現代の代数学はこの本から始まった．邦訳は第 2 版に基づいているが，第 2 版は選択公理を使わないことを公言したことで知られている (第 3 版以降は元へ戻った)．しかし，「つぎつぎ選ぶ」式の記述があちこちに見られ，これが実は選択公理を使っているのだということに当時 (少なくとも一般の数学者は) 気づいていなかった証拠となって残されている．

[2] 彌永昌吉，小平邦彦，現代数学概説 I，岩波書店 (1961)

論理的な厳密性も十分備えた力作 (ただし，チコノフの定理の証明中，選択公理の必要性が明示されていない)．とりわけ加群の理論に詳しい．第 1 章で選択公理，ツォルンの補題，整列原理の同値性も証明されている．集合に関してこれだけ力を注いだ代数系概論は珍しいだろう．この本が出たころ秋月康夫さんが雑誌の座談会で「学部生のうちにこれ位は勉強しておくこと」と話しておられたのを記憶しているが，その当時の学生はそんなに優秀だったかなあ．

[3] 彌永昌吉，布川正巳，代数学，岩波書店 (1968)

広い範囲にわたり渉猟しながらも，演習書のせいもあって記述が簡潔で好ましい．

[4] Jacobson, N., Basic Algebra I, II, Freeman and Co.(2nd edition, 1985)

代数はこれ一冊ですべて済む．読み易く厳密性も申し分ない．ただ，昇鎖律から極大条件を導くに際して "It is easily seen" で済ますとは，これほどの著者にして，どうしたことか．

整数論に関しては以下の通り：

[5] ガウス，整数論 (原著;1801: 高瀬正仁訳；1995，朝倉書店)

19 世紀に聖典視されたガウスの Disquitiones Arithmeticae の高瀬正仁さんによる苦労の翻訳．いくつか文章を引用した．

[6] 高木貞治，初等整数論講義，共立出版 (1931)

文句なく古典．ここまで丁寧に，徹底的に 2 次体の整数論，および 2 次不定方程式論が扱われた本は世界にも珍しいだろう．しかし，手に取るたびに思うのだが，どうして 2 次体のイデアル類群と 2 元 2 次形式類群の同型対応が扱われていないのだろうか．2 次形式類群は数論におけるガウスの主要業績なのに，これが無視されたというのは解せない．「ガウスは無理数を忌避して 2 次形式を専用しているけれども，それは一種の韜晦であって，頭の中では無理数によって構成した理論を発表するのに 2 次形式を籍りたかの感がある．云々」(p.239) は高木先生の読み込みすぎの観がある．この「イデアル重視，2 次形式軽視 (引いては不定方程式軽視)」は後進に少なからず影響を与えたのではないだろうか．

[7] 高木貞治，代数的整数論，岩波書店 (岩波講座数学の一冊として 1935 年に出版された：単行本としての初版は 1947: 第 2 版 1970)

日本で，この本を勉強しなかった整数論研究者は絶無に違いない．しかし，いくらなんでも今どきこの本だけで基礎固めというのでは，現代数学的セン

スに欠けると言われかねない．線型代数学が発達したのは本書が書かれてから後のことだということがよくわかる．また局所解析的な方法もこの本の段階ではまだ未成熟である．なお，これに先立つ 1935 年に岩波講座数学の一冊として出版されているから，初版としては，この年号を挙げるべきではないかと思う．

[8]　稲葉栄治，整数論，共立出版 (1957)

2 次体の整数論を丁寧に扱ってあって，整数論の基礎を勉強するには良い本だと思う．いきなり [7] から勉強し始めるのは，ちょっと実例に関する知識が少なくて後々足元が危険だが，と言っても [6] では手ごわすぎるから，この本あたりから慣れていくのが手頃だろう．

[9]　ボレビッチ，シャハレビッチ，整数論，吉岡書店 (原著；1964：佐々木義雄訳；1971)

イデアル論の代わりに因子論で押し通した珍しい書物．クンマーによって因子 (divisor：クンマーは理想数と呼んだ) が発明され，それがデデキントによってイデアルに書き換えられたのだから，因子論の方が由緒正しいのである．「理想数」は曖昧で難解だったというのは誤伝．クンマーからクロネッカー，ヘンゼルと受け継がれた p 進数論，因子論を発展させたのはハッセの功績である．デデキント，ヒルベルト，高木，アルチンという主流に抗して，生涯，頑なにイデアルという用語の使用を拒んだハッセがこの本をどう評価したのか，一度聞いてみたかった．目的のはっきりしないことが多い日本の教科書とは異なり，不定方程式という観点から主題が選ばれていて，新鮮だった (今でも)．フェルマー予想 (今や定理) を代数的整数論の立場から一通りきちんと扱ったのはこの本だけではなかろうか．ワイルズによってフェルマー予想が解決された現在，代数的整数論の立場からこの問題を詳しく論ずることはなくなるだろうから，そういう意味でも貴重である．訳書は問題に解答が付されていてありがたい．

[10] 石田信，代数的整数論，森北出版 (1974)

主として有理数体上の拡大体に制限して基礎事項を述べてあるので，手軽な厚さにまとまっている．本書にも何箇所か証明を引用した．

[11] 河田敬義，数論——古典数論から類体論へ，岩波書店 (1992)

この本の趣旨は本書 (『類体論へ至る道』) と似ている．しかし，本書の場合は代数と整数論の両方の入門書となることを目標としているから，ずっとレベルは低い．河田さんのこの本には，たとえば，2 次形式類群やハッセ–ミンコウスキーの定理についても詳しく書かれている．代数的整数論の全貌を概観するには良い本であるが，「序論」というには大部で，教科書的である．

[12] 足立恒雄，三宅克哉，類体論講義，日本評論社 (1998)

大局体の類体論をイデアル論とイデール論を併用して証明してから，局所類体論を導いてある．後半の三宅氏の手になる類体論通史は貴重であろう．

[13] 久保田富雄，黒田成勝，整数論，朝倉書店 (1963)

局所体，イデールを含め，基礎事項を網羅してあるのでとても便利．しかしこの本や [10] を含め，代数体の一般論を述べた教科書に共通する難点は，何がどう面白いのか，また目的もあまりよくわからないことである．これは数学の専門書一般の通弊かもしれない．なぜ，たとえば，関連分野の全体像を解説するなり，歴史を記すなり，もう少し面白そうに，広く関心を引き付けられるように書けないのだろうか．最先端まで行かなければ面白い話題はない，というわけではないはずである．しかし，こうした (わからない人にはわかってもらわなくてもよいと言わんばかりの) 独善的傾向も，最近では，異分野との交流を重視する時流の影響か，大分改善されてきているらしいのは喜ばしいことである．

[14] Cassels, Frölich, ed., Algebraic Number Theory, Academic Press (1967)

類体論の整備された現代的教科書の最初のもの．大局体，局所体から始まって，類体論とその周辺が一通りマスターできる．また，ハッセの手になる類体論史が含まれている．ながらくイデアル論が優勢だったが，イデールと

いう happy な概念が発明されたおかげで，歴史の審判は因子論の方に振れたのである，といった趣旨の (「ハッセの勝利宣言」と称すべき) 文章は印象に残る．

選択公理に何度か言及する必要があって，改めて集合論の教科書を何冊か取り出すことになった．それらを中心に挙げておきたい：

[15] Vaught, R.L., Set Theory, Birkhäuser (1985)

素朴集合論と公理的集合論とを行き来しながら書かれた好著．授業で得た知識を使っているからだろうが，証明がわかり易い．しかし，後の方は読みにくくなる．語り口がユニークで面白いから，本書でも何箇所か引用した．

[16] Takeuti, G., Zaring, W.M., Introduction to Axiomatic Set Theory, Springer (1970)

題名通り公理的集合論の入門書である．たとえば,「超限帰納法による関数の定義」など実にていねいに書かれている．竹内さんの他の著書に比べると誤植等がないのは共著者のおかげだろう．

[17] Jech, T., Set Theory, Springer (初版 1978；第 3 版 2002)

巨大な本である．おそらく斯界の聖典なのだろう．素朴な立場から書かれた集合論の本を読んでいると，初心者には何やらわかったようなわからないような気分が残るものだが，この本を読めば，ある程度状況がわかってくれば，結局はきちんと公理主義的に築き上げるのが一番すっきりするのだということが理解できるだろう (これは何も基礎論だけのことではないが)．とにかく，少くとも私には読み易い．もっとも最初の数十ページしか用がないので，後の方のことは知らない．

[18] Fraenkel, A.A. *et al*, Foundations of Set Theory, North-Holland (初版 1958; 改訂版 1973)

集合論の公理化に貢献した一人であるフレンケルが著者の一人に加わっているだけあって，集合論の由来や基礎についてじっくりと書かれた歴史的名

著である．たとえば，等号公理に関する深い考察がこの本にある．本書でも何度か文章を引用した．

[19] 田中尚夫，選択公理と数学——発生と論争，そして確立への道，遊星社 (1987)

選択公理をめぐる歴史や数学については英語でならいくらも優れた著作があるが，日本語ではこの本だけだろう．厚さとしても手頃だが，思想的な深みにまで踏み込んでいるとは言えない (これは日本から出ている他の集合論の教科書についても言える)．そういう文句を言うなら，原書で読めということか．

[20] Henle, J. M., An Outline of Set Theory, Springer (1986；Dover 2007)

一松信さんの訳で『集合論問題ゼミ』(シュプリンガー) として出ていたが現在絶版．しかしドーバー版なら 1000 円代で買える．素人にとって必要十分な集合論の基礎知識とは何かが気になるところだが，この本の最終章を取り去れば，他分野の研究者として，また数学者の教養としてこれだけのことを知っていれば十分だし，必要でもあると言える．ただし，この本だけでマスターできるかどうかは保証しない．あくまで学ぶ目安である．

[21] 足立恒雄，数——体系と歴史，朝倉書店 (2002)

論理から始めて，複素数体まで，本当に厳密な基礎付けができるのかということを自分でチェックしてみたくて書いた本．たとえば，多項式を集合としてどう捉えるかなども明示的に書かれている本というのは少ないだろうと思う．しかし，何分アマチュアの悲しさ，不十分なところが目立つのでいつか改訂できたらと念願している (売れ行きが悪いので，その希望は果たされないままに終わるだろう)．

[22] 難波完爾，数学と論理，朝倉書店 (2003)

難波さんの「地」が良く出た基礎論の概説書．難波さんも，だれにも遠慮せずものを書ける年齢に達したということか．「20 世紀は，結局のところ，有限という素朴な概念が，定義不可能であることを認識するための世紀であっ

たと思う．」(p.32) 難波節ですねェ．「自然数の全体の素朴な定義が，形式的には定義できないのである．」(p.141) というあたり，私が昔から気になっていたことが書かれていて，やっぱりそうなんだ，とうれしかった．「自然数の全体」なんて何のことだか良くわからないのですヨ，本当は！　ただし，証明が付いていないので，素養がないと深く味わうことは困難 (つまり，入門書ではない)．

[23] 上江洲忠弘，集合論・入門，遊星社 (2004)

素朴 (ナイーブ) な立場で書かれているが，ところどころハッとするような個所があって，集合論に疎い私にはとても有意義な本である (しかし，素朴集合論の本の通性で，読み易いとは言えない)．たとえば集合 X, Y について，$X \subseteq Y$ かつ $Y \subseteq X$ であることが $X = Y$ の定義だと思っている人いませんか？　そういう人はこの本を買って読みましょう．(著者もこの勘違いを，以前，上江洲さんに注意されたのだが，この本でやっと納得がいった．ちょっと格好の悪い話だが，標準的な数学者はそんなものだという証拠として書いておく．)　数学の非操作性に言及した「あとがき」は味わい深い．「線は無限個の点でできているというのですね．$\cdots$ それでは，その線から一つだけで良いから点を取り出して私に見せてくれませんか $\cdots$」だって．

索　引

数字・アルファベット

ア　行

カ　行

サ　行

タ　行

ナ　行

ハ　行

足立恒雄（あだち・のりお）

略歴

1941 年 京都府福知山市に生まれる.

1965 年 早稲田大学理工学部数学科を卒業.

現　在　早稲田大学理工学術院教授．理学博士.

主な著書

専門書

『フェルマーの大定理——整数論の源流』（日本評論社，ちくま学芸文庫），『フェルマーを読む』，『数論——歴史からのアプローチ』（共訳），『類体論講義』（共著），『ガロア理論講義』（以上，日本評論社），『理工基礎　微分積分学 I』，『理工基礎　微分積分学 II』（サイエンス社），『数——体系と歴史』（朝倉書店）

一般書

『無限の果てに何があるか』（光文社カッパ・サイエンス，光文社知恵の森文庫），『$\sqrt{2}$ の不思議』（光文社カッパ・サイエンス，ちくま学芸文庫），『フェルマーの大定理が解けた！』，『無限のパラドクス』（以上，講談社ブルーバックス），『「無限」の考察』（講談社）

類体論へ至る道——初等数論からの代数入門［改訂新版］

1979 年 12 月 15 日　第 1 版　第 1 刷発行

2010 年　2 月 25 日　改訂新版第 1 刷発行

著　者　足　立　恒　雄

発行者　黒　田　敏　正

発行所　株式会社　日　本　評　論　社

〒170-8474 東京都豊島区南大塚 3-12-4

電話　(03) 3987-8621［販売］

(03) 3987-8599［編集］

印　刷　藤原印刷株式会社

製　本　松岳社

装　幀　林 健造

ISBN 978-4-535-78643-1

類体論講義　日評数学選書

足立恒雄・三宅克哉／著

類体論は現代代数学で必須の基礎知識であるが、その体系の壮大さと証明の難しさのため、やさしい入門書が皆無であった。
本書は、長い講義経験をもとに書き下ろされた待望の入門書である。
詳細な歴史もあわせて収録。

◇ISBN978-4-535-60125-3／A5判／312ページ／定価4,515円（税込）

数論 ── 歴史からのアプローチ

アンドレ・ヴェイユ／著　足立恒雄・三宅克哉／訳

シモーヌ・ヴェイユの実兄であり、現代数学に指導的役割を果たしてきたアンドレ・ヴェイユが渾身の力をこめて書き下ろした名著の完訳。
ヴェイユの数学史観を知るのに好適の講演「数学史」も併せて収録した。

◇ISBN978-4-535-78160-3／菊判／402ページ／定価7,875円（税込）

ガロワ理論《上》

デイヴィッド・A.コックス／著　梶原健／訳

代数学の基礎や歴史的背景、折り紙・作図問題やレムニスケートなど、ガロワ理論をめぐるさまざまな話題を盛り込んだ入門書の上巻。

◇ISBN978-4-535-78454-3／菊判／284ページ／定価3,675円（税込）

日本評論社　http://www.nippyo.co.jp/